(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年4 月15 日 (15.04.2004)

PCT

(10) 国際公開番号
WO 2004/031941 A1

(51) 国際特許分類[7]: G06F 7/58

(21) 国際出願番号: PCT/JP2003/012213

(22) 国際出願日: 2003 年9 月25 日 (25.09.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-285168 2002 年9 月30 日 (30.09.2002) JP
特願2003-101085 2003 年4 月4 日 (04.04.2003) JP
特願2003-294101 2003 年8 月18 日 (18.08.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ＦＤＫ株式会社 (FDK CORPORATION) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 Tokyo (JP).

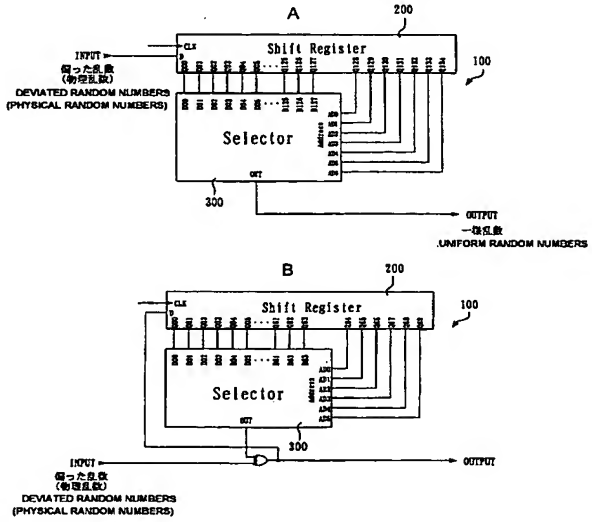
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 山本 博康 (YAMAMOTO,Hiroyasu) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). ビターナゲ アナンダ (VITHANAGE,Ananda) [LK/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 清水 隆邦 (SHIMIZU,Takakuni) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 藤田 香 (FUJITA,Kaoru) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 中野 初美 (NAKANO,Hatsumi) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 志賀 隆明 (SHIGA,Takaaki) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 曽我 竜司 (SOGA,Ryuji) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 上遠野 昌良 (KATONO,Masayoshi) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 渡邊 利幸 (WATANABE,Toshiyuki) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP). 鯉渕 美佐子 (KOIBUCHI,Misako) [JP/JP]; 〒105-0004 東京都 港区 新橋５丁目３６番１１号 ＦＤＫ株式会社内 Tokyo (JP).

[続葉有]

(54) Title: METHOD OF UNIFORMING PHYSICAL RANDOM NUMBER AND PHYSICAL NUMBER GENERATION DEVICE

(54) 発明の名称: 物理乱数の一様化手法と物理乱数発生装置



(57) Abstract: A method of uniforming physical random numbers, capable of maintaining a random number generating velocity and ensuring security concurrently. The method sequentially inputs a plurality of physical random numbers to a shift register to hold them there, and shifts them every time a reference pulse signal rises. Physical random numbers held in the shift register are randomly selected and output by a selector based on part of them. Accordingly, physical random numbers input to the shift register are uniformed and then output even thought they have a deviation, thereby eliminating the chance of not outputting random numbers or letting others recognize the deviation of random numbers.

[続葉有]

WO 2004/031941 A1

(74) 代理人: 清水 千春, 外(SHIMIZU,Chiharu et al.); 〒104-0061 東京都 中央区 銀座８丁目１６番１３号 中銀・城山ビル４階 Tokyo (JP).

(81) 指定国 (国内): CN, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供する。本発明によれば、複数の物理乱数をシフトレジスタに順次入力して保持し、基準パルス信号が立ち上がるごとにシフトする。シフトレジスタに保持された物理乱数をその一部に基づいてセレクタでランダムに選択して出力する。これにより、シフトレジスタに入力された物理乱数は、それが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に知られる事態が起きない。

明 細 書

物理乱数の一様化手法と物理乱数発生装置

技 術 分 野

本発明は、偏りのある物理乱数を簡単に一様化することが可能な物理乱数の一様化手法に関するものである。

更に、本発明は、各種の用途に用いるに好適な物理乱数発生装置に関するものであり、その具体的な用途としては、セキュリティー、暗号、認証、施錠、暗号化通信、スマートカード（例えば、電子マネー、クレジットカード、診察券）、ホームセキュリティー、カーセキュリティー、キーレスエントリー、確率、抽選、ゲーム、アミューズメント（例えば、パチンコ、パチスロ）、シミュレーション（例えば、気象・学術計算・株価におけるモンテカルロ）、グラフィックス（例えば、ＣＧ、自動作曲）、制御、計測、ＦＡ、ロボット制御（人工知能）などが挙げられる。

背 景 技 術

一般に乱数には、計算によって決定論的に生成される擬似乱数と、自然界の物理現象を利用して生成される物理乱数とがある。後者（物理乱数）は真の意味でランダムな現象を基に生成されるので、理想的な乱数となる資質があるものの、実際に物理乱数を生成する場合、途中過程で様々な誤差要因が介在するため、必ずしも理想的な乱数が出力されるとは限らず、偏りのある乱数が出てきてしまう恐れもある。この誤差要因としては、デジタル化の際に基準となるクロックの幅や、ノイズを利用する場合に余計なノイズが混入することなどが挙げられる。

従来、こうした物理乱数の偏りを改善する手法、すなわち物理乱数の一様化手法としては、２つの２進乱数を用いて乱数の偏りを改善するノイマンコレクター（例えば、非特許文献１参照）や、ノイズに基づいて発生させた物理乱数を擬似乱数と合成することで物理乱数の偏りを改善する手法（以下、乱数合成法と称す

る。）が提案されていた（例えば、特開２００１－３４４０９４号公報（段落〔００１４〕および〔００１８〕の欄および図１参照、また、非特許文献であるBenjamin Jun and Paul Kocher著、"The Intel Random Number Generator"、CRYPTOGRAPHY RESEARCH、１９９９年４月２２日発表（第４頁、4.3.Digital Post-Processing）参照。）

しかし、ノイマンコレクターでは、１ビットの乱数を出力するのに２ビットの乱数を必要とする上に、その２ビットの組合せによっては乱数を出力しない場合もあるので、乱数の発生速度が落ちてしまう欠点があった。

また、乱数合成法では、擬似乱数がわかれば、基になる物理乱数を出力から取り出せるようになるため、乱数の偏りが他人に知られてしまい、保安性に欠けるという不都合があった。

また、前記したような従来の物理乱数発生装置としては、半導体内で発生するノイズを用いたものが多く、パソコンに外部から接続して使用するよう構成される規模の大きなものや、ＩＣチップ単体で乱数を発生させるものがあった。また、アミューズメント用には、時間的にランダムであると見なせる信号が発生した時に、備えられた高速カウンターの値を参照し、それを乱数として用いるものがあった。

一般に物理乱数発生器は高速に乱数を発生することは難しく、時としてその乱数発生速度以上の大量の乱数が必要となる事が起こる。そのため、記憶媒体を設けて乱数を貯めておいたり、複数の物理乱数発生装置を用いで乱数の発生量を増やしたりすることが考えられるが、これを実現するためには複雑な回路を利用者側で組む必要が生じる。

また、一般に物理乱数は使用環境によって乱数の質が変化する可能性があり、利用者がこれら物理乱数発生装置の発生した乱数が真正乱数として使用することができるか否かを確認することは有益なことである。しかしながら、乱数の検定を行うには専用の測定装置を構築しなければならず、一般の物理乱数発生装置利用者にとっては、このような余計なコストと手間がかかるような作業は受け入れ難い。また、乱数検定は大量のデータを扱うので、それを貯めておく記憶装置は大容量のものが必要となるとともに、検定のための計算処理にも時間がかかる。

更に、従来の物理乱数発生装置としては、例えば特開２００３－２９９６４号公報に開示されているように、２個のディレーおよびセレクター等からなる位相調整部と、フリップ・フロップと、フィードバック回路とから構成される物理乱数発生器を備えたものが知られている。

しかし、これでは、フリップ。フロップのクロック端子とデータ端子に入力される２系統の信号ラインに応じた２個のディレーおよびセレクタが必要となるので、位相調整部、ひいては物理乱数発生器の規模が大きくなり、その占有面積が拡大するばかりか、その消費電力が増大するという不都合があった。特に、物理乱数発生器がＣＰＵ（中央演算処理装置）、ＲＯＭ（読取り専用記憶装置）、ＲＡＭ（読取り書き込み記憶装置）などの多くの機能とＩＣ（集積回路）内に混載される場合には、この物理乱数発生器の専有面積をできる限り縮小することが強く望まれる。

発　明　の　開　示

本発明は、このような事情に鑑み、乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供することを目的とする。

本発明の他の目的は、物理乱数発生装置単体での乱数利用効率が高く、かつ複数の物理乱数ＩＣを組み上げて乱数を高速に発生させることが容易であり、さらに、乱数の質を容易に確認して使用することが可能な物理乱数発生装置を提供せんとするものである。

更に、本発明の別の目的は、占有面積が小さくて消費電力が少ない物理乱数発生器と、この物理乱数発生器が組み込まれた物理乱数発生装置を提供せんとするものである。

先ず、本発明のうち、請求項１に係る発明は、複数の物理乱数を乱数保持装置（２００）に入力して保持し、この乱数保持装置に保持された物理乱数の一部をセレクターのアドレスとして使用し、そのアドレスに基づいて残りの部分から乱数をランダムに選択して出力することを特徴とする物理乱数の一様化手法である。

また、本発明の請求項２に係る発明は、前記セレクターに代え、論理積回路を

用い乱数保持装置に保持された乱数をランダムに選択して、それらの排他的論理和を出力することを特徴とする物理乱数の一様化手法である。

更に、本発明の請求項３に係る発明は、セレクターの出力と物理乱数を入力とする排他的論理和回路を設けその出力を乱数保持装置（２００）入力とする請求項１に記載の物理乱数の一様化手法である。

また、本発明の請求項４に係る発明は、請求項１から請求項３の何れかの操作を２サイクル以上繰り返して物理乱数を多段に一様化することを特徴とする物理乱数の一様化手法である。

また、本発明の請求項５に係る発明は、乱数保持装置としてシフトレジスタ（２００）を用いたことを特徴とする請求項１から請求項４までのいずれかに記載の物理乱数の一様化手法である。

なお、括弧内の符号は図面において対応する要素を表す便宜的なものであり、したがって、本発明は図面上の記載に限定拘束されるものではない。このことは「特許請求の範囲」の欄についても同様である。

次に、本発明のうち請求項６に係る発明は、物理乱数発生器を有する物理乱数発生装置であって、前記物理乱数発生器が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、パラレル乱数を保持しうる複数個のレジスターを備え、前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えて構成される。ここで、読出しクロックは基準クロックとは別に入力されるものである。

また、本発明のうち請求項７に係る発明は、前記物理乱数発生器が、複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ／ダウンカウンターを備え、前記アップ／ダウンカウンターが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、前記セレクターからのロード

信号に基づいて前記シリアル／パラレル変換部内のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスターへ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスターより前段にある各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えて構成される。

また、本発明のうち請求項８に係る発明は、前記物理乱数発生器が、前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンターを備え、前記総数カウンターがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路を備えて構成される。

また、本発明のうち請求項９に係る発明は、前記乱数検証回路の乱数検証方法として、乱数値“０”又は“１”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

また、本発明のうち請求項１０に係る発明は、前記乱数検証回路の乱数検証方法として、４ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出されたχ二乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

また、本発明のうち請求項１１に係る発明は、前記乱数検証回路の乱数検証方法として、連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

また、本発明のうち請求項１２に係る発明は、前記乱数検証回路の乱数検証方法として、所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

また、本発明のうち請求項１３に係る発明は、チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファー機能を３ステートとして構成される。

さらに、本発明のうち請求項１４に係る発明は、前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力するようにして構成される。

さらに、本発明のうち請求項１５に係る発明は、抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路と、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力する増幅器と、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを２個ずつ備え、前記各エッジ検出回路の出力信号の位相差に基づいて”０”または”１”を出力するフリップ・フロップを備え、前記各積分回路に入力される入力信号の位相を調整するディレー、第１セレクターおよびアップ／ダウンカウンターからなる位相調整部を備え、前記フリップ・フロップから出力される”０”または”１”がそれぞれ５０％に収束するように当該フリップ・フロップの出力を前記位相調整部にフィードバックするフィードバック回路を備えた物理乱数発生器において、前記各積分回路の前段にそれぞれ第２セレクター及び第３セレクターを設け、前記アップ／ダウンカウンターの最上位ビットによって前記第１セレクターと前記第２セレクターおよび前記第３セレクターとの入力の極性切換を行う極性切換回路を設けたことを特徴とする物理乱数発送器である。

さらに、本発明のうち請求項１６に係る発明は、抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路を１個備え、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを２個ずつ備え、前記各エッジ検出回路の出力信号の位相差に基づいて”０”または”１”を出力するフリップ・フロップを備えた物理乱数発生器において、前記フリップ・フロップに入力される入力信号の位相を調整するディレーとセレクターからなる可変ディレーを前記各エッジ検出回路の前段または後段に設け、前記フリップ・フロップから出力される”０”または”１”がそれぞれ５０％に収束するように当該フリップ・フロップの出力を前記可変ディレーにフィードバックするフィードバック回路を設けたことを特徴とする物理乱数発生器である。

さらに、上記構成において、前記積分回路の抵抗の後段にＦＥＴ（電界効果トランジスタ）を当該積分回路のキャパシタと並列に付加した構成とすることもで

きる。

また、上記構成の前記積分回路の抵抗に代えて、定電流回路を設けた構成とすること可能である。

図面の簡単な説明

図１Ａおよび図１Ｂは、本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の二例を示す回路図である。

図２Ａ及び図２Ｂは、本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の別の二例を示す回路図である。

図３Ａ及び図３Ｂは、本発明に係る物理乱数の一様化手法が適用される乱数一様化回路のさらに別の二例を示す回路図である。

図４は本発明に係る物理乱数発生装置の第１の実施形態を示す回路図。

図５は図４に示す物理乱数発生装置の物理乱数発生器の詳細を示す回路図。

図６は図５に示す物理乱数発生器の各部の出力波形を示す波形図。

図７は図５に示す物理乱数発生器の各部の出力波形を示す波形図。

図８は図４に示す物理乱数発生装置の乱数検証回路のMonobitTestに関する部分の回路図。

図９は図４に示す物理乱数発生装置の乱数検証回路のPokerTestに関する部分の回路図。

図１０は図４に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図。

図１１は図４に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図。

図１２は図４に示す物理乱数発生装置の乱数検証回路のLongRunsTestに関する部分の回路図である。

図１３は本発明に係る物理乱数発生装置の第２の実施形態を示す回路図。

図１４は本発明に係る物理乱数発生装置の第３の実施形態を示す回路図。

図１５は図１４に示す物理乱数発生装置の各部の出力波形を示す波形図。

図１６は本発明の係る物理乱数発生器の別の実施形態を示す回路図。

図１７は図１６に示す物理乱数発生器のエッジ検出回路の詳細を示す図。

図１８は図１６に示す物理乱数発生器の動作波形を示す図。

図１９は本発明に係る物理乱数発生器の更に別の実施形態を示す回路図。

図２０は積分回路の別の例を示す回路図。

図２１は図２０に示す積分回路を用いた物理乱数発生器の動作波形を示す図。

図２２は積分回路の更に別の例を示す図であり、更に

図２３は、図２２に示す積分回路を用いた物理乱数発生器の動作波形を示す図である。

発明を実施するための最良の形態

＜発明の第１の態様＞

以下、本発明の実施形態を図面に基づいて説明する。

まず、図１Ａに示す乱数一様化回路１００では、シフトレジスタ２００とセレクタ３００とを具備しており、シフトレジスタ２００のデータ端子Ｄには２進乱数（「０」または「１」）が順次入力され、シフトレジスタ２００のクロック端子ＣＬＫに入力される基準パルス信号が立ち上がるごとに、これらの２進乱数が順に出力Ｑ００～Ｑ１３４にシフトされていく。そして、シフトレジスタ２００の出力Ｑ００～Ｑ１２７の１２８ビットの乱数はそれぞれセレクタ３のデータ端子Ｄ００～Ｄ１２７に入力され、シフトレジスタ２００の出力Ｑ１２８～Ｑ１３４の７ビットの乱数はそれぞれセレクタ３００のアドレスＡＤ０～ＡＤ６に入力される。

その後、セレクタ３００では、アドレスＡＤ０～ＡＤ６に入力された７ビットのアドレス値に応じて、データ端子Ｄ００～Ｄ１２７に入力された１２８ビットの乱数から１ビットが選択され、出力端子ＯＵＴから出力される。例えば、アドレスＡＤ０～ＡＤ６にそれぞれ「１」「０」「０」「０」「０」「０」「０」が入力されたときは、データ端子Ｄ００に入力された乱数が出力端子ＯＵＴから出力される。また、アドレスＡＤ０～ＡＤ６にそれぞれ「１」「０」「１」「０」「０」「０」「０」が入力されたときは、データ端子Ｄ０４に入力された乱数が出力端子ＯＵＴから出力される。

このように、シフトレジスタ２００のデータ端子Ｄに順次入力される２進乱数は、その一部がアドレスとなって自分自身をランダムに選び出すので、この２進乱数が偏りを持っていても、この乱数一様化回路１で一様化されて出力されることになる。しかも、従来のノイマンコレクターと異なり、１ビットの乱数を出力するのに複数ビットの乱数を必要とすることもなく、乱数を出力しない場合もないため、乱数の発生速度を維持することができる。また、従来の乱数合成法と違って、乱数の偏りが他人に知られてしまう事態が生じないので、保安性を確保することができる。

また、図１Ｂに示す乱数一様化回路１００は、シフトレジスタ２００からの乱数出力を選択するビット数を６ビットに減らしたことと、排他的論理和（ＸＯＲ）回路を追加したことを除き、図１Ａに示す乱数一様化回路１と同様である。すなわち、図１Ｂに示す乱数一様化回路１では、シフトレジスタ２００とセレクタ３００とを具備しており、セレクタ３００の出力と２進乱数（「０」または「１」）とを入力とする排他的論理和回路の出力が順次シフトレジスタ２００のデータ端子Ｄに入力され、シフトレジスタ２００のクロック端子ＣＬＫに入力される基準パルス信号が立ち上がるごとに、出力Ｑ００～Ｑ６９に順にシフトされていく。そして、シフトレジスタ２００の出力Ｑ００～Ｑ６３の６４ビットの乱数はそれぞれセレクタ３００のデータ端子Ｄ００～Ｄ６３に入力され、シフトレジスタ２の出力Ｑ６４～Ｑ６９の６ビットの乱数はそれぞれセレクタ３００のアドレスＡＤ０～ＡＤ５に入力される。その後、セレクタ３００では、アドレスＡＤ０～ＡＤ５に入力された６ビットのアドレス値に応じて、データ端子Ｄ００～Ｄ６３に入力された６４ビットの乱数から１ビットが選択され、出力端子ＯＵＴから出力される。

この場合も、シフトレジスタ２００のデータ端子Ｄに順次入力される２進乱数は、その一部がアドレスとなって自分自身をランダムに選び出すので、この２進乱数が偏りを持っていても、この乱数一様化回路１００で一様化されて出力されることになり、乱数の発生速度を維持すると同時に、保安性を確保することができる。

このことを確認するため、この乱数一様化回路１００から出力された乱数の一

様性を乱数検定規格ＦＩＰＳ１４０－２に準拠して評価した。その結果を表１および表２に示す。なお、表１中の数値は元データを表し、表２中の数値は検定結果データを表す。ここで、表１、２中の「Ｍｏｎｏ」、「Ｐｏｋｅｒ」、「Ｒｕｎｓ」および「ＬｏｎｇＲｕｎ」は乱数検定の種類を表しており、それぞれ乱数検定規格ＦＩＰＳ１４０－２の「Monobit Test」、「Porker Test」、「Runs Test」および「Long Run Test」に対応している。また、結果は５０回を１セットとして表示しており、数値は５０回の検定中で不合格になった回数を表している。

【表１】

セットNo.	Mono	Poker	Runs	LongRun
1	0	0	1	0
2	0	0	0	0
3	0	0	1	0
4	0	0	1	0
5	0	0	1	0
6	0	0	2	0
7	0	0	0	0
8	0	0	0	0
9	0	0	1	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	1	0
15	0	0	0	0
16	0	0	1	0
17	0	0	1	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	1	1
22	0	0	1	0
23	0	0	1	0
24	0	0	0	0
25	0	0	0	0
26	0	0	1	0
27	0	0	0	0
28	0	0	0	0
29	0	0	1	0
30	1	0	0	0
31	0	0	0	1
32	0	0	1	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	1
36	0	0	1	0
37	0	0	1	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	0	0
42	0	0	0	0
43	0	0	1	0
44	0	0	0	0
45	0	0	0	0
46	0	0	2	0
47	0	0	0	0
48	0	0	1	0
49	0	0	0	0
50	0	0	0	0

【表２】

セットNo.	Mono	Poker	Runs	LongRun
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	1	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0
27	0	0	0	0
28	0	0	0	0
29	0	0	0	0
30	0	0	0	0
31	0	0	0	0
32	0	0	0	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	0
36	0	0	0	0
37	0	0	0	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	1	0
42	0	0	0	0
43	0	0	0	0
44	0	0	0	0
45	0	0	0	0
46	0	0	0	0
47	0	0	0	0
48	1	0	0	0
49	0	0	0	0
50	0	0	0	0

上に示した表１及び表２から明瞭に理解させるように、４種類すべての乱数検定（「Ｍｏｎｏ」、「Ｐｏｋｅｒ」、「Ｒｕｎｓ」および「ＬｏｎｇＲｕｎ」）において、セットNo.１～５０のほとんど全部が合格値となり、上述した効果が確認された。

一方、図２Ａに示す乱数一様化回路１は、シフトレジスタ２００からの乱数出力を選択するビット数を１５ビットに増やしたことと、セレクタ３００と同様な働きをするものとして論理積（ＡＮＤ）回路と排他的論理和（ＸＯＲ）回路との組み合わせを代用したことを除き、図１Ａに示す乱数一様化回路１と同様である。すなわち、図２Ａに示す乱数一様化回路１ではシフトレジスタ２００を具備しており、シフトレジスタ２００のデータ端子Ｄには２進乱数（「０」または「１」）が順次入力され、シフトレジスタ２００のクロック端子ＣＬＫに入力される基準パルス信号が立ち上がるごとに、これらの２進乱数が順に出力Ｑ００～Ｑ３０にシフトされていく。そして、シフトレジスタ２００の出力Ｑ００～Ｑ１４の１５ビットの乱数とシフトレジスタ２００の出力Ｑ１６～Ｑ３０の１５ビットの乱数とを入力とする１５個の論理積回路の出力が、シフトレジスタ２００の出力Ｑ１５とともに排他的論理和回路で順次合成されて出力される。

このように、シフトレジスタ２００のデータ端子Ｄに順次入力される２進乱数は、シフトレジスタ２００内で同じビット数（１５ビット）の２組に分けられた後、論理積回路と排他的論理和回路でランダムに演算されるので、この２進乱数が偏りを持っていても、この乱数一様化回路１で一様化されて出力されることになる。しかも、従来のノイマンコレクターと異なり、１ビットの乱数を出力するのに複数ビットの乱数を必要とすることもなく、乱数を出力しない場合もないため、乱数の発生速度を維持することができる。また、従来の乱数合成法と違って、乱数の偏りが他人に知られてしまう事態が生じないので、保安性を確保することができる。

また、図２Ｂに示す乱数一様化回路１００は、シフトレジスタ２００からの乱数出力を選択するビット数を７ビットに減らしたことと、排他的論理和（ＸＯＲ）回路を追加したことを除き、図２Ａに示す乱数一様化回路１と同様である。すなわち、図２Ｂに示す乱数一様化回路１ではシフトレジスタ２００を具備してお

り、シフトレジスタ２００のデータ端子Ｄには２進乱数（「０」または「１」）が順次入力され、シフトレジスタ２００のクロック端子ＣＬＫに入力される基準パルス信号が立ち上がるごとに、これらの２進乱数が順に出力Ｑ００～Ｑ１４にシフトされていく。そして、シフトレジスタ２の出力Ｑ００～Ｑ０６の７ビットの乱数とシフトレジスタ２の出力Ｑ０８～Ｑ１４の７ビットの乱数とを入力とする７個の論理積回路の出力が、シフトレジスタ２００の出力Ｑ０７とともに排他的論理和回路で順次合成され、最後に元の２進乱数（生データ）と排他的論理和回路で合成されて出力される。

この場合も、シフトレジスタ２００のデータ端子Ｄに順次入力される２進乱数は、シフトレジスタ２００内で同じビット数（７ビット）の２組に分けられた後、論理積回路と排他的論理和回路でランダムに演算されるので、この２進乱数が偏りを持っていても、この乱数一様化回路１００で一様化されて出力されることになり、乱数の発生速度を維持すると同時に、保安性を確保することができる。

なお、上述の実施形態においては、複数の物理乱数を保持する乱数保持装置としてシフトレジスタ２００を用いた場合について説明したが、シフトレジスタ２００以外の乱数保持装置（例えば、フリップフロップ）を代用することも可能である。

また、上述の実施形態においては、１個の乱数一様化回路１を用いて物理乱数を一様化する場合について説明したが、図３Ａ及び図３Ｂに示すように、図１Ａ、図１Ｂや図２Ａ、図２Ｂに示す乱数一様化回路１００　（ＣＫＴ１，ＣＫＲ２，・・・ＣＫＴｘ）を２個以上接続して物理乱数を多段に一様化することもできる。この場合、乱数一様化回路１００の接続方法は、図３Ａに示すような直列接続であっても、図３Ｂに示すような並列接続であっても構わない。

以上説明したように、本発明によれば、乱数保持装置（シフトレジスタ）に入力された物理乱数は、たとえそれが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に知られてしまう事態が起きないことから、乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供することができる。

＜発明の第２の態様＞

次に、本発明の物理乱数発生器の好適な実施例について図面の図４～図１５を参照して説明する。

この物理乱数発生装置９１は、図４に示すように、物理乱数発生器１、乱数検証回路２１、制御回路９４、カウンター９５、第１セレクター９６、第２セレクター９７から構成されており、物理乱数発生器１は、図５に示すように、シリアル物理乱数発生器２、カウンター３、シフトレジスター４、複数個（図５ではm個）のレジスター５、制御回路６、アップ／ダウンカウンター７、セレクター８、基準クロック側の２個の遅延回路９および読出しクロック側の２個の遅延回路１０から構成されている。

他方、乱数検証回路２１は、図８から図１２までに示すように、乱数検定規格ＦＩＰＳ１４０－２に準拠した４種類の検定方法（MonobitTest、PokerTest、RunsTestおよびLongRunsTest）に対応する部分から構成されている。すなわち、MonobitTestに関する部分は、図８に示すように、第１カウンター２３、第２カウンター２４、レジスター２５、制御回路２６および比較器２７から構成されており、PokerTestに関する部分は、図９に示すように、第１カウンター３３、シフトレジスター３４、デコーダー３５、複数個（図９では１６個）のカウンター３６、制御回路３７、セレクター３８、掛算器３９、加算器４０、レジスター４１および比較器４２から構成されている。また、RunsTestに関する部分はさらに乱数出力が“１”の場合と乱数出力が“０”の場合とに二分され、前者は、図１０に示すように、第１カウンター５３、比較器５４、データ保持器５５、第２カウンター５６、制御回路５７、デコーダー５８、６個のカウンター５９および６個の比較器６０から構成されており、後者は、図１１に示すように、物理乱数発生器１のシリアル物理乱数発生器２からデコーダー５８への出力線上にインバータが設けられて出力が反転する点を除き、前者と同じ構成を有している。さらに、LongRunsTestに関する部分は、図１２に示すように、第１カウンター７３、比較器７４、データ保持器７５、制御回路７６、第２カウンター７７、第１比較器７８、レジスター７９および第２比較器８０から構成されている。

物理乱数発生装置９１は以上のような構成を有するので、この物理乱数発生装

置９１を作動させると、まず物理乱数発生器１で、シリアル乱数が出力されるとともに、パラレル乱数が保持されて必要に応じて出力できる状態となる。

すなわち、基準クロック(CLK_0)でシリアル物理乱数発生器２より生成されたシリアル乱数(SRND)をカウンター３のキャリーアウト(CO)に同期して、シフトレジスター４でシリアルからパラレルに変換したｎビットの乱数(CRND)をセレクター８で選択されたレジスター５にロードしてパラレル乱数を保持する。

このとき、セレクター８はアップ／ダウンカウンター７の出力の書込みアドレス(ADDRESS)で指定されたレジスター５を選択し、カウンター３のキャリーアウト(CO)に同期してパラレル乱数(CRND)をレジスター５にロードし、ロードごとにアップ／ダウンカウンター７をカウントアップし、アップ／ダウンカウンター７の出力の書込みアドレス(ADDRESS)がｍになった時点で、アップ／ダウンカウンター７はカウントアップとパラレル乱数のロードを中止し、以降その状態を維持する。

パラレル乱数の出力(PRND)は最下位のレジスター５の出力とし、読み出し後に読出しクロック(CLK_R)を入力し、読出しクロックにてアップ／ダウンカウンター７のカウントダウンとすべてのレジスター５内のデータを上位から下位へシフトし、パラレル乱数(PRND)はその都度更新される。アップ／ダウンカウンター７の出力の書込みアドレス(ADDRESS)がゼロになった時点で、アップ／ダウンカウンター７はカウントダウンとデータシフトを中止し、以降その状態を維持する。

アップ／ダウンカウンター７の出力の書込みアドレス(ADDRESS)は外部に出力され、すべてのレジスター５に保持されているパラレル乱数の数を逐次モニター可能とする。

遅延回路９、１０は各クロックのエッジ（例えば、立上りエッジ）を取り出し、非常に短いパルス波形（例えば、１０ｎｓ）を生成し、アップ／ダウンカウンター７とすべてのレジスター５のクロック信号(CLOCK)、アップ／ダウンカウンター７のENABLE信号、すべてのレジスター５のSHIFT信号とLOAD(0)～LOAD(m-1)を生成する。これにより、基準クロック(CLK_0)と読出しクロック(CLK_R)が非同期または同期式で動作するときに、基準クロック(CLK_0)のエッジ（例えば、立上りエッジ）に対する読出しクロック(CLK_R)のエッジ（例えば、立上りエッジ

）の禁止域(td_Ra+td_0a+２×td_mg)を非常に小さくして基準クロック(CLK_0)と読出しクロック(CLK_R)との干渉を最小限とすることができる。なお、CLK_0bとCLK_Rbがクロック信号(CLOCK)を生成し、CLK_0aとCLK_RaがENABLE信号、SHIFT信号とLOAD(0)～LOAD(m-1)を生成する。

制御回路６はカウンター３のキャリーアウト(CO)の同期信号(SYNC)、CLK_0a、CLK_Ra、アップ／ダウンカウンター７のOVER信号とZERO信号より、アップ／ダウンカウンター７のUP/DOWN信号とENABLE信号、すべてのレジスター５のSHIFT信号とLOAD(0)～LOAD(m-1)用のLOAD信号を生成する。

こうすることにより、基準クロックに同期してシリアル物理乱数発生器２で生成されたシリアル乱数よりｎ倍の周期で最大m個のｎビットのパラレル乱数を保持することができる。それ以降のシリアル乱数は読み出し操作（CLK_Rの入力）をするまでは保持されない。こうして保持された最大m個のパラレル乱数は読出しクロックで必要なときに必要な量（最大m個）を短時間に集中して読み出すことができ、読み出された量のパラレル乱数は逐次補充される。基準クロック(CLK_0)のエッジに対する読出しクロックのエッジの禁止域が非常に狭く、非同期または同期式でタイミングよく、かつ効率的に読み出すことができる。書込みアドレスを読み出すことで、その時点で保持されたパラレル乱数の量を確認することが可能となり、乱数を効率的に活用することができる。

ところで、こうしてシリアル物理乱数発生器２で生成されたシリアル乱数は、乱数検定規格ＦＩＰＳ１４０－２に準拠した４種類の検定方法（MonobitTest、PokerTest、RunsTestおよびLongRunsTest）でその一様性が検証される。

まず、MonobitTestによる検証が行われる。すなわち、図８に示すように、第１カウンター２３はスタート信号(START)と基準クロック(CLK_0)より制御回路２６を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。第２カウンター２４は制御回路２６の出力信号CLR_C2でスタート信号(START)が入った時点に初期化を行い、シリアル乱数(SRND)の“１”または“０”をカウントする。レジスター２５は制御回路２６の出力信号LOAD_Rでスタート信号(START)が入った時点より20,000クロック時の第２カウンター２４のカウント値をロードして保持し、MonobitData(MOND)を出力する。比較器２

７はレジスター２５の出力MonobitData(MOND)と上限比較データ（例えば、10,275bit）および下限比較データ（例えば、9,725bit）とを比較し、MonobitJudge(MONJ)信号を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にMonobitDataとMonobitJudgeを検証することができる。

次に、PokerTestによる検証が行われる。すなわち、図９に示すように、第１カウンター３３はスタート信号(START)と基準クロック(CLK_0)より制御回路３７を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。シフトレジスター３４はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次４ビットのパラレル乱数(PRND_4B)に変換する。デコーダー３５は、スタート信号(START)と基準クロック(CLK_0)より制御回路３７を介して生成されたENABLE信号がアクティブのとき（４クロックごとに１回）にパラレル乱数(PRND_4B)で指定された出力部(SE_0～SE_15)に出力される。カウンター３６は制御回路３７の出力信号CLR_CRでスタート信号(START)が入った時点に初期化を行い、ENABLE信号がアクティブのとき（４クロックごとに１回）にパラレル乱数(PRND_4B)のデータにてデコーダー３５で指定されたカウンター３６をカウントアップする。すべてのカウンター３６の総計は5,000カウントとなり、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にその間の４ビットごとのパラレル乱数(PRND_4B)のデータ（０～１５）の度数分布データ(PokerData0～PokerData15)を取得する。レジスター４１は、制御回路３７の出力信号CLR_CRでスタート信号(START)が入った時点に初期化(POKD=0)を行い、度数分布データ(PokerData0～PokerData15)を取得した後、セレクター３８、掛算器３９、加算器４０を介して度数分布データ(PokerData0～PokerData15)の１６個の二乗和を求めることでPokerData(POKD)を取得する。比較器４２はレジスター４１の出力PokerData(POKD)と上限比較データ（例えば、1,576,928）および下限比較データ（例えば、1,563,175）とを比較し、PokerJudge(POKJ)信号を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000+16クロック後にPokerDataとPokerJudgeを検証することができる。

次いで、RunsTestによる検証が行われる。すなわち、図１０および図１１に示すように、第１カウンター５３はスタート信号(START)と基準クロック(CLK_0)より制御回路５７を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。データ保持器５５はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次１ビット保持し、比較器５４はシリアル乱数(SRND)とデータ保持器５５で保持された乱数を比較し、１クロック前の乱数と今回の乱数が変化したときに信号CHANGEを出力する。第２カウンター５６は、信号CHANGEが出力されてから次の出力がされるまでのクロックをカウントし、信号RUNS_Dを出力する。信号RUNS_Dと同一信号の長さ(L)の関係はL=RUNS_D+1となる。第２カウンター５６は、制御回路５７の出力信号CLR_CCでスタート信号(START)が入ったときと信号CHANGEが出力されたときに初期化(RUNS_D=0)を行う。デコーダー５８は、スタート信号(START)、基準クロック(CLK_0)、第１カウンター５３の出力(OUT_C)と比較器５４の出力(CHANGE)より制御回路５７を介して生成されたENABLE信号がアクティブ（CHANGEがアクティブ）のときで、図１０ではシリアル乱数(SRND)が“１”のとき、図１１ではシリアル乱数(SRND)が“０”のとき、第２カウンター５６の出力(RUNS_D)で選択された出力(SE_1～SE_6+)をアクティブにする。なお、L=1→SE_1、L=2→SE_2、…、L=6+→SE_6+となる。すべてのカウンター５９は、制御回路５７の出力信号CLR_Cでスタート信号(START)が入った時点に初期化を行い、デコーダー５８の出力(SE_1～SE_6+)で指定されたカウンター５９をカウントアップし、１～６＋の同一信号の長さ(L)の出現回数（図１０ではRunsData1H～RunsData6+H、図１１ではRunsData1L～RunsData6+L）を取得する。各比較器６０は各カウンター５９の出力（図１０ではRunsData1H～RunsData6+H、図１１ではRunsData1L～RunsData6+L）とそれぞれの上限比較データ（例えば、2,685、1,386、723、384、209、209）および下限比較データ（例えば、2,315、1,114、527、240、103、103）とを比較し、判定信号（図１０ではRunsJudge1H～RunsJudge6+H、図１１ではRunsJudge1L～RunsJudge6+L）を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にRunsTestのデータと判定を検証することができる。

最後に、LongRunsTestによる検証が行われる。すなわち、図１２に示すように

、第１カウンター７３はスタート信号(START)と基準クロック(CLK_0)より制御回路５７を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。データ保持器７５はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次１ビット保持し、比較器７４はシリアル乱数(SRND)とデータ保持器７５で保持された乱数を比較し、１クロック前の乱数と今回の乱数が変化したときに信号CHANGEを出力する。第２カウンター７７は、信号CHANGEが出力されてから次の出力がされるまでのクロックをカウントし、信号LRUNS_Dを出力する。第２カウンター７７は、制御回路７６の出力信号CLR_CCでスタート信号(START)が入ったときと信号CHANGEが出力されたときに初期化(LRUNS_D=0)を行う。レジスター７９は、制御回路７６の出力信号CLR_Rでスタート信号(START)が入ったときに初期化(LRUNS_D=0)を行う。レジスター７９の出力信号LongRunsData(LRND)と第２カウンター７７の出力信号(LRUNS_D)を第１比較器７８で比較し、LRND＜LRUNS_Dのときに第１比較器７８は出力信号COMP_Uを出力し、制御回路７６を介してレジスター７９にLOAD_R信号を出力して、レジスター７９に逐次LRUNS_Dの最大値を保持する。第２比較器８０は上限比較データ（例えば、26）と比較し、判定信号LongRunsJudge(LRNJ)を出力する。信号LRUNS_D、LRNDと同一信号の長さ(L)の関係はL=LRUNS_D+1、L(max)=LRND+1=LRUNS_D(max)+1となる。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にLongRunsTestのデータと判定を検証することができる。

そして、こうして４種類の検定方法で検証された一様性乱数の検証データは、図４に示すように、第２セレクター９７に保持され、使用者の要望に応じて出力される。選択信号(A0、A1)と動作テーブルを表３に示す。

【表３】

ADDRE_S	A1	A0	読出しクロック(CLK_R)の働き	出力(DATA BUS)
0	0	0	パラレル物理乱数の更新	パラレル物理乱数
1	0	1	パラレル物理乱数の更新	パラレル物理乱数の生成状態
2	1	0	乱数検証のスタート／カウンターの初期化	乱数検証状態／モニターアドレス
3	1	1	乱数検証のモニターアドレス更新	乱数検証結果／検証データ

すなわち、物理乱数発生器１は、選択信号(A1)の状態（“０”または“１”）

により、読出しクロック(CLK_R)でのパラレル乱数の更新（アップ／ダウンカウンター７のカウントダウン）または非更新とする。出力のパラレル乱数(PRND)は第２セレクター９７のDATA_0に接続される。出力(COND_R)には書込みアドレス(ADDRESS)などの物理乱数生成時およびパラレル乱数変換時に生成される各種データやフラグを出力し、第２セレクター９７のDATA_1に接続される。

乱数検証回路２１は、選択信号(A0、A1)が２(ADDRE_S)のときに制御回路９４を介して読出しクロック(CLK_R)信号で検証を開始し、MonobitTest、PokerTest、RunsTestおよびLongRunsTestを基準クロック(CLK_0)で20,000+16サイクルで完了し、判定結果、判定データ、PokerTestの生データを出力して第１セレクター９６に接続される。その詳細を表４に示す。

【表４】

モニターアドレス(SEL_ADD)	出力(DATA BUS)
0	0 ; Monobit Judge(MONJ) 1 ; Poker Judge(POKJ) 2 ; Runs Judge 1H(RUNJ1H) 3 ; Runs Judge 1L(RUNJ1L) 4 ; Runs Judge 2H(RUNJ2H) 5 ; Runs Judge 2L(RUNJ2L) 6 ; Runs Judge 3H(RUNJ3H) 7 ; Runs Judge 3L(RUNJ3L) 8 ; Runs Judge 4H(RUNJ4H) 9 ; Runs Judge 4L(RUNJ4L) 10 ; Runs Judge 5H(RUNJ5H) 11 ; Runs Judge 5L(RUNJ5L) 12 ; Runs Judge 6+H(RUNJ6+H) 13 ; Runs Judge 6+L(RUNJ6+L) 14 ; Long Run Judge(LRNJ) 15 ; 総合判定
1	Monobit Data(MOND)
2	Poker Data(POKD)
3	Runs Data 1H(RUND1H)
4	Runs Data 1L(RUND1L)
5	Runs Data 2H(RUND2H)
6	Runs Data 2L(RUND2L)
7	Runs Data 3H(RUND3H)
8	Runs Data 3L(RUND3L)
9	Runs Data 4H(RUND4H)
10	Runs Data 4L(RUND4L)
11	Runs Data 5H(RUND5H)
12	Runs Data 5L(RUND5L)
13	Runs Data 6+H(RUND6+H)
14	Runs Data 6+L(RUND6+L)
15	Long Run Data(LRND)
16	Poker Data 0 (POK_0)
17	Poker Data 1 (POK_1)
18	Poker Data 2 (POK_2)
19	Poker Data 3 (POK_3)
20	Poker Data 4 (POK_4)
21	Poker Data 5 (POK_5)
22	Poker Data 6 (POK_6)
23	Poker Data 7 (POK_7)
24	Poker Data 8 (POK_8)
25	Poker Data 9 (POK_9)
26	Poker Data 10 (POK_10)
27	Poker Data 11 (POK_11)
28	Poker Data 12 (POK_12)
29	Poker Data 13 (POK_13)
30	Poker Data 14 (POK_14)
31	Poker Data 15 (POK_15)

なお、総合判定はすべての判定結果が合格のときに出力される。出力(COND_T)には、乱数検証時に生成される各種データやフラグを出力し、第２セレクター９７のDATA_2にカウンター出力のモニターアドレス(SEL_ADD)とともに接続される。また、検証のスタート信号にてパラレル乱数生成用のカウンター３、シフトレジスター４、アップ／ダウンカウンター７とすべてのレジスター５は初期化され、検証された物理乱数を保持して検証後の物理乱数を使用することができる。

カウンター９５は第１セレクター９６のモニターアドレス(SEL_ADD)を生成する。カウンター９５は、制御回路９４の出力信号(CLR_C)で選択信号(A0、A1)が２(ADDRE_S)のときに読出しクロック(CLK_R)信号で検証を開始し、この開始時に初期化を行い、制御回路９４の出力信号(CLK_C)で選択信号(A0、A1)が３(ADDRE_S)のときに読出しクロック(CLK_R)信号でカウンター９５のカウントアップ（更新）を行う。

これにより、基準クロックに同期して生成されたシリアル乱数(SRND)と逐次補充されるパラレル乱数(PRND)の生成及び一様性の検証を逐次行うことができる。

こうすることにより、物理乱数発生器１の検証およびデータの確認が容易となり、検証後の乱数を活用することができる。選択信号(A0、A1)と第２セレクター９７を用いることで入出力端子を大幅に減らすことができる。選択信号(A0、A1)、読出しクロック(CLK_R)、カウンター９５と第２セレクター９７で、参照できる有効な検証データを拡大することができる。

なお、図１３に示すように、物理乱数発生器１にチップセレクト(CS)と出力イネーブル(OE)の入力を付加し、パラレル乱数[PRND(0)～PRND(n-1)]の出力形態を３ステート（“０”、“１”、off）にすることもできる。

また、図１４および図１５に示すように、複数個（図１４ではｐ個）の物理乱数発生器１とセレクター１２とで高速（図１４ではｐ倍）の乱数生成スピードを獲得することも可能である。ここで、基準クロック(CLK_0)のエッジ（例えば、立上りエッジ）に対する読出しクロック(CLK_R)のエッジ（例えば、立上りエッジ）の禁止域(td_Ra+td_0a+２×td_mg)を非常に狭く考慮することのみで非同期または同期式の高速乱数発生を容易に実現することができる。

このように、チップセレクト(CS)と出力イネーブル(OE)を有することで、物理

乱数発生器１を複数個接続することが容易となり、乱数生成の高速化が可能となる。また、チップセレクト(CS)と出力イネーブル(OE)を有することで、ＣＰＵを使用したシステムに物理乱数発生器１を容易に接続することができる。

なお、上述の実施形態では、基準クロック(CLK_0)のエッジに対する読出しクロック(CLK_R)のエッジの禁止域(td_Ra+td_0a+２×td_mg)を非常に小さくして基準クロック(CLK_0)と読出しクロック(CLK_R)との干渉を最小限とするため、基準クロック側および読出しクロック側にそれぞれ２個の遅延回路９、１０を設けた場合について説明したが、基準クロック側と読出しクロック側のいずれか一方にだけ遅延回路９、１０を設けてもよく、遅延回路９、１０の個数も１個以上であれば何個でも構わない。或いはまた、遅延回路９、１０に代えて波形成形回路（例えば、単安定マルチバイブレータ）を付加しても、同じ効果を得ることができる。

以上説明したように、本発明の上記第２の態様のうち請求項４～１０に係る発明によれば、生成された物理乱数を効率よく利用することができるとともに、その乱数の一様性を容易に検定して使用することができ、かつ、簡単な回路構成によりこれらを実現することが可能となる。

また、本発明の第２の態様のうち請求項１１および１２に係る発明によれば、複数個の物理乱数発生ＩＣを用いて高速に乱数を発生させることが容易となり、かつ、Data Busに直接接続できるようになるため、物理乱数発生装置の使い易さが格段に向上する。

＜発明の第３の態様＞

本発明の更に別の実施態様において、図１６および図１８に示すように、抵抗Ｒおよびキャパシタ（コンデンサ）Ｃでクロック信号を積分して積分波形を出力する積分回路１０５と、ノイズ源１０６と、このノイズ源１０６のノイズを増幅してノイズ信号を出力する増幅器１０７と、積分波形とノイズ信号とをミキシングするミキサー１０８と、このミキサー１０８の出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路１０９とが２個ずつ設けられている。各エッジ検出回路１０９は、図１７に示すような回路構成となっており、これらのエッジ検出回路１０９の後段には、図１６に示すように、各エッジ検

出回路１０９の出力信号の位相差に基づいて”０”または”１”を出力するＤタイプのフリップ・フロップ１１０が設けられている。更に、フリップ・フロップ１１０の後段には、乱数をクロック信号に同期させるＤタイプのフリップ・フロップ１１１が設けられている。

また、物理乱数発生器１０１の最前段には、各積分回路１０５に入力される入力信号の位相を調整する位相調整部１０２が設けられており、この位相調整部１０２はディレー１２１、第１セレクター１２２及びアップ／ダウンカウンター１２３から構成されている。

また、フリップ・フロップ１１１の出力とアップ／ダウンカウンター１２３との間にはフィードバック回路１０３が設けられており、フリップ・フロップ１１１～出力される”０”または”１”がそれぞれ５０％に収束するようにフリップ・フロップ１１１の出力が位相調整部１０２にフィードバックされる。すなわち、フィードバック回路１０３は第１カウンター１３１、比較器１３２，第２カウンター１３３，レジスター１３４，比較器１３５，シフトレジスター／レジスター１３６、加算機１３７から構成されており、第１カウンター１３１および比較器１３２はフィードバックの周期を乱数（２×ｍ）で生成する。また、第２カウンター１３３、レジスター１３４および比較器１３５はフィードバックの周期（２×ｍ）中の”０”または”１”の数をカウント（ｎ）し、比較データをアップ／ダウンカウンター１２３に出力して乱数の一様性を補正するフィードバック信号を出力する。さらに、シフトレジスタ／レジスター１３６および加算機１３７は、フィードバックの周期を決める乱数（ｍ）を出力（ＯＵＴ）より取得する。これにより、フィードバック周期による乱数の質の低下（癖）を　防ぐことができる。

さらに、位相調整部１０２各積分回路１０５との間にはそれぞれ第２セレクター１１５および第３セレクター１１６が設けられていると共に、第１セレクター１２２とアップ／ダウンカウンター１２３との間には極性切換回路１１３が設けられており、表５に示すように、アップ／ダウンカウンター１２３の最上位ビットＭＳＢによって第１セレクター１２２と第２セレクター１１５および第３セレクター１１６との入力の極性切換が行われる。

【表５】

アップ/ダウンカウンター	SELECT	第1セレクターのアドレス	第2セレクターの出力	第3セレクターの出力	相対的な時間差
1Fh	1	1Fh	0(A)	P-1(A)	P
1Eh	1	1Eh	0(A)	P-2(A)	P-1
⋮	1	⋮	⋮	⋮	⋮
02h	1	02h	0(A)	2(A)	3
01h	1	01h	0(A)	1(A)	2
00h	1	00h	0(A)	0(A)	1
3Fh	0	00h	0(B)	-1(B)	0
3Eh	0	01h	1(B)	-1(B)	-1
⋮	0	02h	2(B)	-1(B)	-2
⋮	0	⋮	⋮	⋮	⋮
22h	0	⋮	⋮	⋮	⋮
21h	0	1Eh	P-2(B)	-1(B)	-P+2
20h	0	1Fh	P-1(B)	-1(B)	-P+1

したがって、２系統の信号ラインに応じた２個のディレーおよびセレクターを必要とする従来の物理乱数発生器と比べて、ディレー１２１及び第１セレクター１２２を半分にしてゲート数を削減することができるので、物理乱数発生器１０１の規模を小さくして占有面積を縮小し、その消費電力を低減することが可能となる。

図１９は本発明の更に別の実施例による物理乱数発生器の回路図である。この物理乱数発生器１０１においては、図１９に示すように、抵抗Ｒおよびキャパシタ Ｃでクロック信号を積分して積分波形を出力する積分回路１０４が１つ設けられていると共に、ノイズ源１０６と、このノイズ源１０６のノイズを増幅してノイズ信号を出力する増幅器１０７と、積分波形とノイズ信号とをミキシングするミキサー１０８と、このミキサー１０８の出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路１０９とが２個ずつ設けられている。これらのエッジ検出回路１０９の後段には、各エッジ検出回路９の出力信号の

位相差に基づいて”０”または”１”を出力するＤタイプのフリップ・フロップ１１０が設けられており、フリップ・フロップ１１０の後段には、乱数をクロック信号に同期させるＤタイプのフリップ・フロップ１１０が設けられている。

また、フリップ・フロップ１１０と各エッジ検出回路１０９との間（各エッジ検出回路１０９の後段）にはそれぞれ、ディレーとセレクターからなる可変ディレー１１９が設けられており、フリップ・フロップ１１０に入力される入力信号の位相を調整することができる。

さらに、フリップ・フロップ１１１の出力とアップ／ダウンカウンター１２３との間にはフィードバック回路１０３が設けられており、フリップ・フロップ１１１から出力される”０”または”１”がそれぞれ５０％に収束するようにフリップ・フロップ１１１の出力が可変ディレー１１９にフィードバックされる。

したがって、２系統の信号ラインについて積分回路１０５が１つで済むことに加えて、積分回路１０５を構成する抵抗Ｒ、キャパシタＣの誤差による位相調整範囲を狭めることができるため、ディレーとセレクターからなる可変ディレー１１９を縮小し、ゲート数を削減することができることから、物理乱数発生器１０１の規模を小さくして占有面積を縮小し、その消費電力を低減することが可能となる。

尚、上記の第１９図に示した実施形態において、図２０に示すように、積分回路１０５の抵抗Ｒの後段にＦＥＴ（電界トランジスタ）１１７をキャパシタＣと並列に付加してもよい。この場合は、図２１に示すように、積分回路１０５のキャパシタＣに充電された電荷を放電して電位を積分波形の基点に戻すことにより、積分波形の基点が常に安定し、その結果としてジッターの分布も安定する。さらに、ジッターの分布が安定することは良質な乱数を生成することにつながる。また、乱数生成は電位が基点に戻るまで待たなければならないが、積分回路１０５のキャパシタＣに充電された電荷が高速に放電され、電位も高速に積分波形の基点に戻るため、乱数生成までの待ち時間を短縮することができる。それに加え、乱数生成後に波形の電位が上がりきるのを待たずして強制的に基点まで電位を下げることができるので、さらなる時間短縮が可能となる（乱数生成したら、すぐに電位を基点まで戻せる）。これにより、乱数生成スピードを大幅に高速化す

ることができる。同様に、上述した図１６～図１８に示した実施形態において、各積分回路１０５の抵抗Ｒの後段にＦＥＴ１１７をキャパシタＣと並列に付加することもできる。

また、上記図１９に示した実施形態において、図２２に示すように、積分回路１０５の抵抗Ｒに代えて、定電流回路１１８も設けても構わない。この場合は、図２３に示すように、キャパシタＣの充電時の積分波形が直線となり、ノイズに対して変調したジッターの歪みがなくなるため、乱数の質が向上する。同様に、上述した図１６～図１８の実施形態において、各積分回路１０５の抵抗Ｒに代えて定電流回路１１８を設けることも可能である。

また、図３Ｂの実施例について説明したと同様に、上述した物理乱数発生器１０１をｋ個（ｋは２以上の数値）並列に接続し、各物理乱数発生器１０１に入力されたパラレル物理乱数をｋ個のシリアル物理乱数に並べ替え、排他的論理和（ＸＯＲ）素子を介して出力することにより、複数個の物理乱数発生器１０１からなる物理乱数発生装置の乱数の質を向上させることができる。

また、図１６～図１８の実施形態及び図１９の実施形態においては、乱数発生用のフリップ・フロップとしてＤタイプのフリップ・フロップを用いた場合について説明したが、本発明ではこれに限定されるわけではなく、これと同等の機能を有するフリップ・フロップであれば代用できる。

また、図１９の実施形態においては、図示の如く、ディレーとセレクターからなる可変ディレー１１９をエッジ検出回路１０９の後段に設けた場合について説明したが、可変ディレー１１９をエッジ検出回路１０９の前段に設けてもよい。

請 求 の 範 囲

1．複数の物理乱数を乱数保持装置（２００）に入力して保持し、この乱数保持装置に保持された物理乱数の一部をセレクターのアドレスとして使用し、そのアドレスに基づいて残りの部分から乱数をランダムに選択して出力することを特徴とする物理乱数の一様化手法。

2．前記セレクターに代え、論理積回路を用い乱数保持装置に保持された乱数をランダムに選択して、それらの排他的論理和を出力することを特徴とする物理乱数の一様化手法。

3．セレクターの出力と物理乱数を入力とする排他的論理和回路を設けその出力を乱数保持装置（２００）入力とする請求項１に記載の物理乱数の一様化手法。

4．請求項１から請求項３の何れかの操作を２サイクル以上繰り返して物理乱数を多段に一様化することを特徴とする物理乱数の一様化手法。

5．乱数保持装置としてシフトレジスタ（２００）を用いたことを特徴とする請求項１から請求項４までのいずれかに記載の物理乱数の一様化手法。

6．物理乱数発生器を有する物理乱数発生装置であって、該物理乱数発生器が、

基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、

シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、

パラレル乱数を保持しうる複数個のレジスターを備え、

前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えたことを特徴とする物理乱数発生装置。

7．前記物理乱数発生器が、

複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ／ダウンカウンターを備え、

前記アップ／ダウンカウンターが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、

前記セレクターからのロード信号に基づいて前記シリアル／パラレル変換部内のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスターへ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスターより前段にある各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えたことを特徴とする請求項４に記載の物理乱数発生装置。

8．前記物理乱数発生器が、

前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンターを備え、

前記総数カウンターがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路を備えたことを特徴とする請求項６または請求項７に記載の物理乱数発生装置。

9．前記乱数検証回路の乱数検証方法として、

乱数値“０”または“１”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項８に記載の物理乱数発生装置。

１０．前記乱数検証回路の乱数検証方法として、

４ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出されたχ二乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法

を採用したことを特徴とする請求８に記載の物理乱数発生装置。

１１．前記乱数検証回路の乱数検証方法として、

連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項８に記載の物理乱数発生装置。

１２．　前記乱数検証回路の乱数検証方法として、

所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項８に記載の物理乱数発生装置。

１３．チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファー機能を３ステートとしたことを特徴とする請求項６から請求項１２までのいずれかに記載の物理乱数発生装置。

１４．前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力するようにしたことを特徴とする請求項６から請求項１３までのいずれかに記載の物理乱数発生装置。

１５．抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路と、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力する増幅器と、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを２個ずつ備え、

前記各エッジ検出回路の出力信号の位相差に基づいて”０”または”１”を出力するフリップ・フロップを備え、

前記各積分回路に入力される入力信号の位相を調整するディレー、第１セレク

ターおよびアップ／ダウンカウンターからなる位相調整部を備え、

前記フリップ・フロップから出力される”０”または”１”がそれぞれ５０％に収束するように当該フリップ・フロップの出力を前記位相調整部にフィードバックするフィードバック回路を備えた物理乱数発生器において、

前記各積分回路の前段にそれぞれ第２セレクター及び第３セレクターを設け、

前記アップ／ダウンカウンターの最上位ビットによって前記第１セレクターと前記第２セレクターおよび前記第３セレクターとの入力の極性切換を行う極性切換回路を設けたことを特徴とする物理乱数発送器。

１６．抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路を１個備え、

ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを２個ずつ備え、

前記各エッジ検出回路の出力信号の位相差に基づいて”０”または”１”を出力するフリップ・フロップを備えた物理乱数発生器において、

前記フリップ・フロップに入力される入力信号の位相を調整するディレーとセレクターからなる可変ディレーを前記各エッジ検出回路の前段または後段に設け、

前記フリップ・フロップから出力される”０”または”１”がそれぞれ５０％に収束するように当該フリップ・フロップの出力を前記可変ディレーにフィードバックするフィードバック回路を設けたことを特徴とする物理乱数発生器。

１７．前記積分回路の抵抗の後段にＦＥＴ（電界効果トランジスタ）を当該積分回路のキャパシタと並列に付加したことを特徴とする請求項１５又は請求項１６の物理乱数発生器。

１８．前記積分回路の抵抗に代えて、定電流回路を設けたことを特徴とする請求

項１５から請求項１７までのいずれかに記載の物理乱数発生器。

１９．請求項１５から請求項１８までのいずれかに記載の物理乱数発生器を２個以上並列接続し、前記各物理乱数発生器に入力されたパラレル物理乱数をシリアル物理乱数に並べ替えて出力するようにした物理乱数発生装置。

FIG. 1A

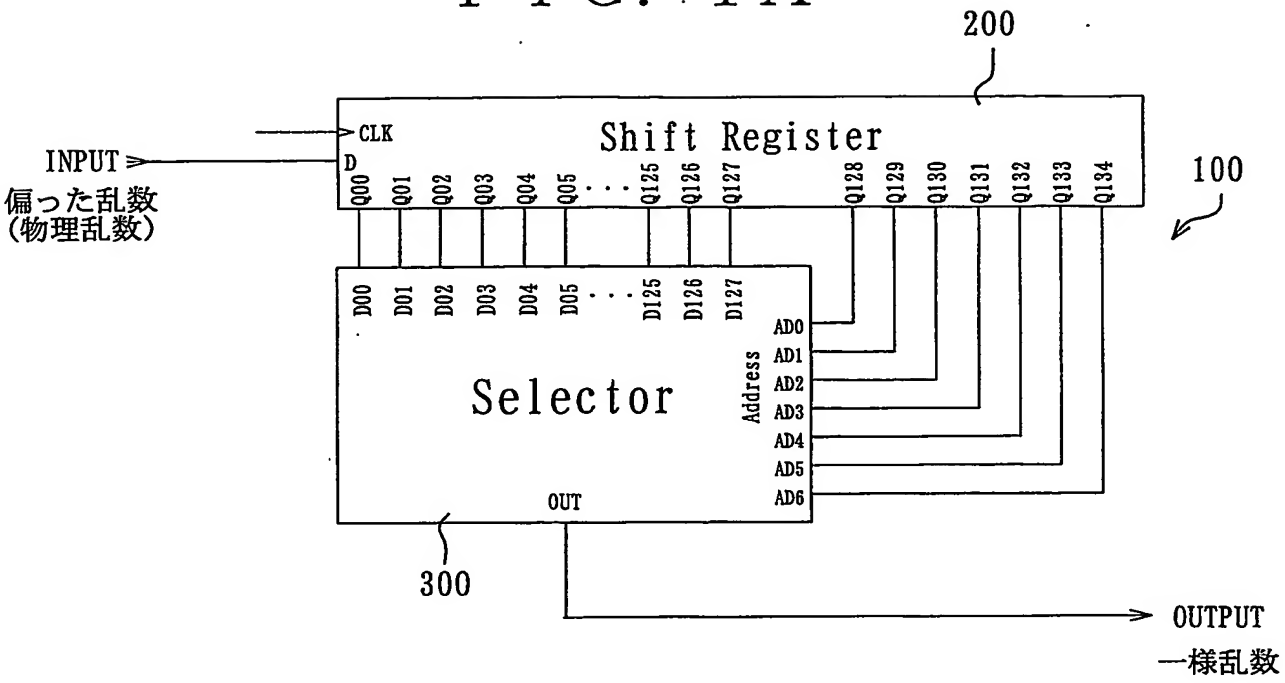

200
Shift Register
CLK
D
INPUT
偏った乱数
(物理乱数)
Q00 Q01 Q02 Q03 Q04 Q05 ... Q125 Q126 Q127 Q128 Q129 Q130 Q131 Q132 Q133 Q134
100
D00 D01 D02 D03 D04 D05 ... D125 D126 D127
Selector
Address
AD0 AD1 AD2 AD3 AD4 AD5 AD6
OUT
300
OUTPUT
一様乱数

FIG. 1B

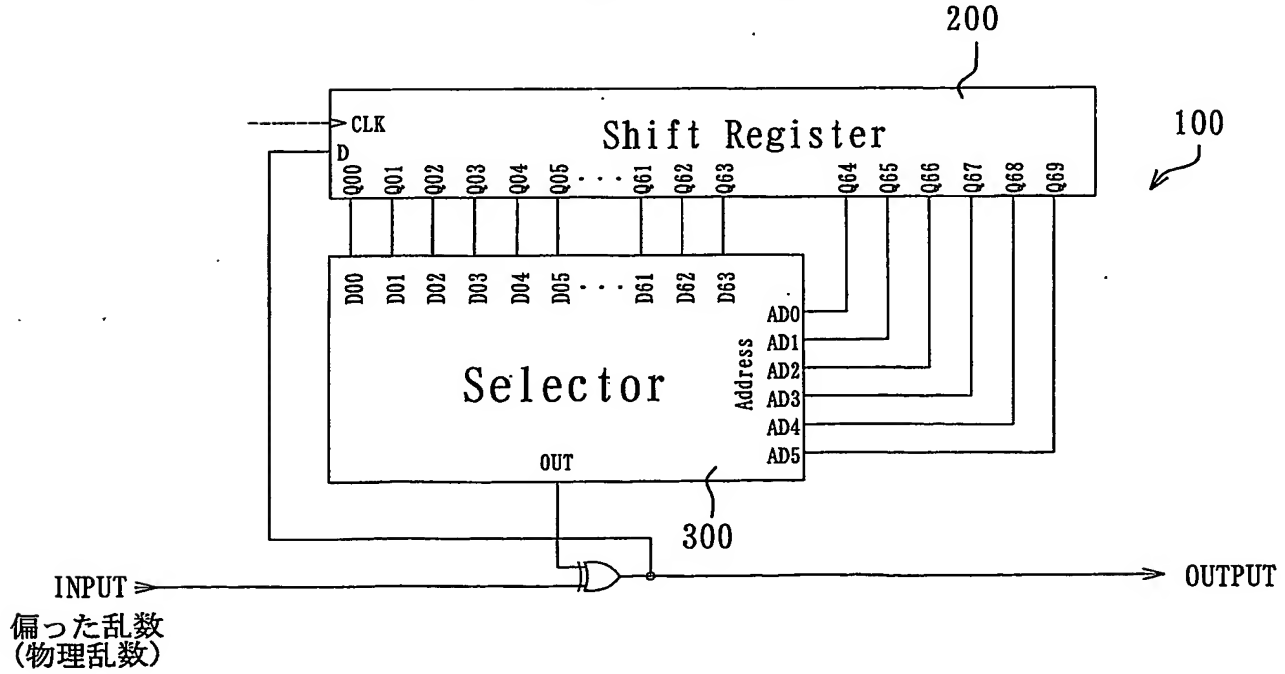

200
Shift Register
CLK
D
Q00 Q01 Q02 Q03 Q04 Q05 ... Q61 Q62 Q63 Q64 Q65 Q66 Q67 Q68 Q69
100
D00 D01 D02 D03 D04 D05 ... D61 D62 D63
Selector
Address
AD0 AD1 AD2 AD3 AD4 AD5
OUT
300
INPUT
偏った乱数
(物理乱数)
OUTPUT

FIG. 2A

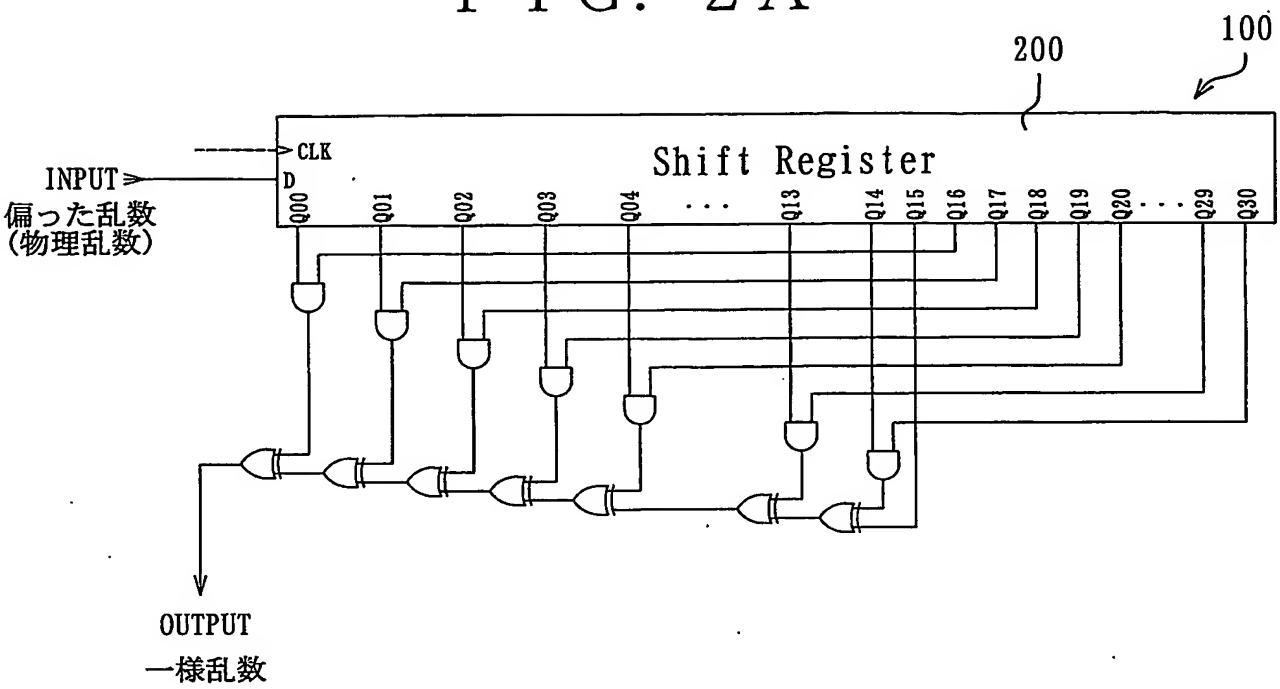

100
200
Shift Register
CLK
D
INPUT
偏った乱数
(物理乱数)
Q00
Q01
Q02
Q03
Q04
Q13
Q14
Q15
Q16
Q17
Q18
Q19
Q20
Q29
Q30
OUTPUT
一様乱数

FIG. 2B

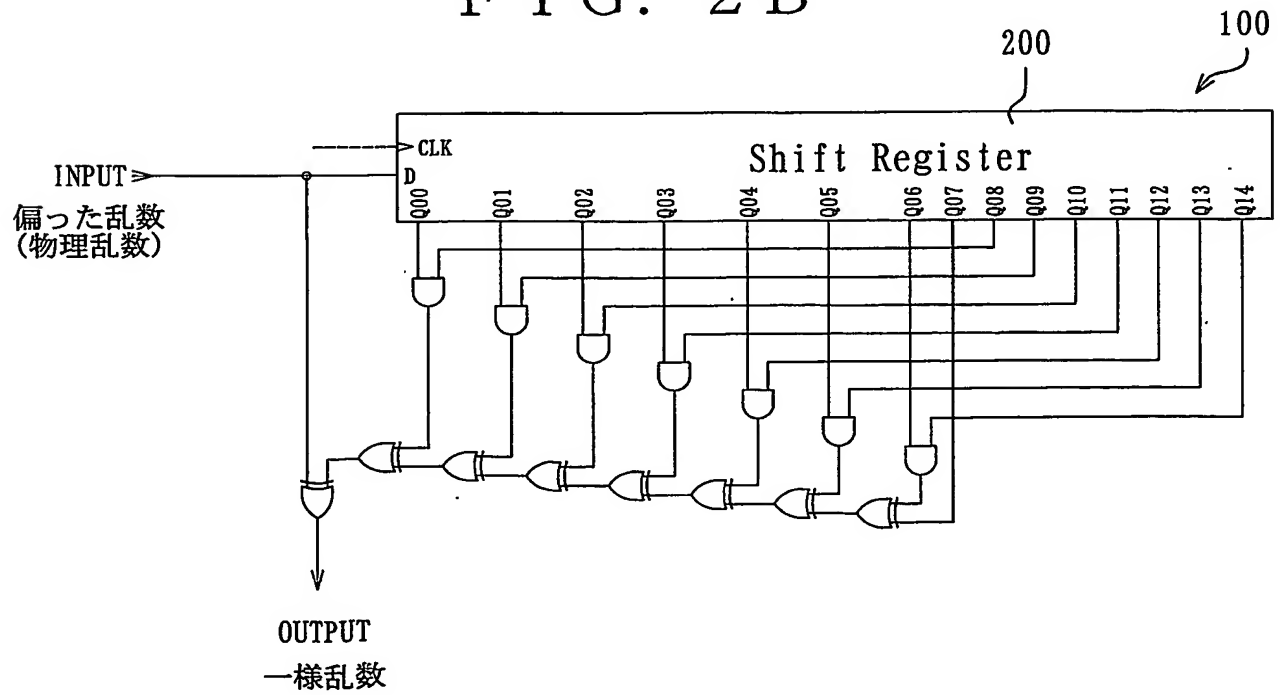

100
200
Shift Register
CLK
D
INPUT
偏った乱数
(物理乱数)
Q00
Q01
Q02
Q03
Q04
Q05
Q06
Q07
Q08
Q09
Q10
Q11
Q12
Q13
Q14
OUTPUT
一様乱数

FIG. 3A

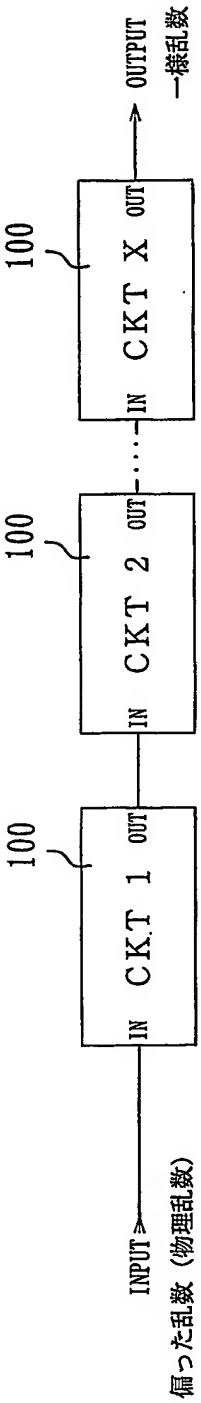

100
IN CKT 1 OUT
100
IN CKT 2 OUT
100
IN CKT X OUT
INPUT
偏った乱数（物理乱数）
OUTPUT
一様乱数

FIG. 3B

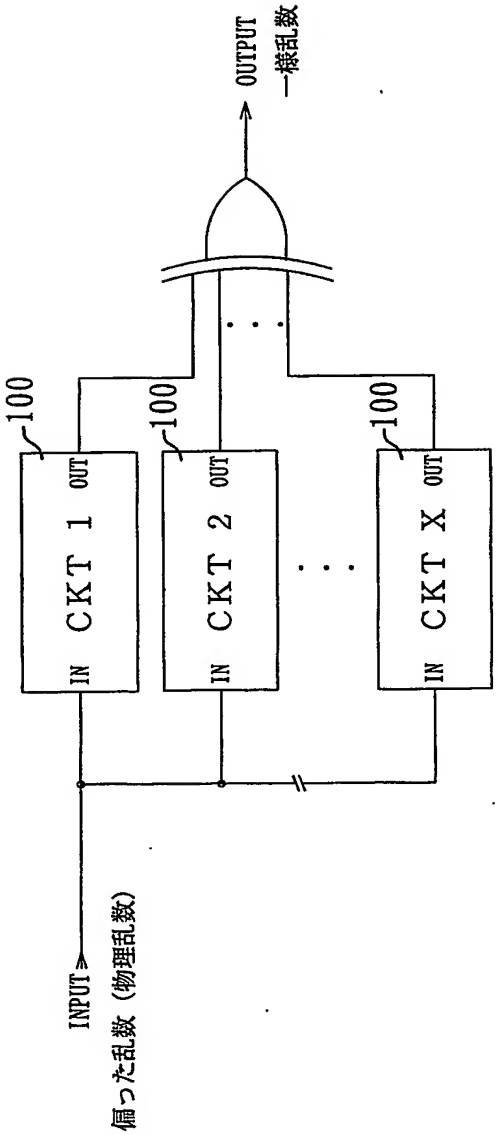

100
IN CKT 1 OUT
100
IN CKT 2 OUT
100
IN CKT X OUT
INPUT
偏った乱数（物理乱数）
OUTPUT
一様乱数

FIG. 4

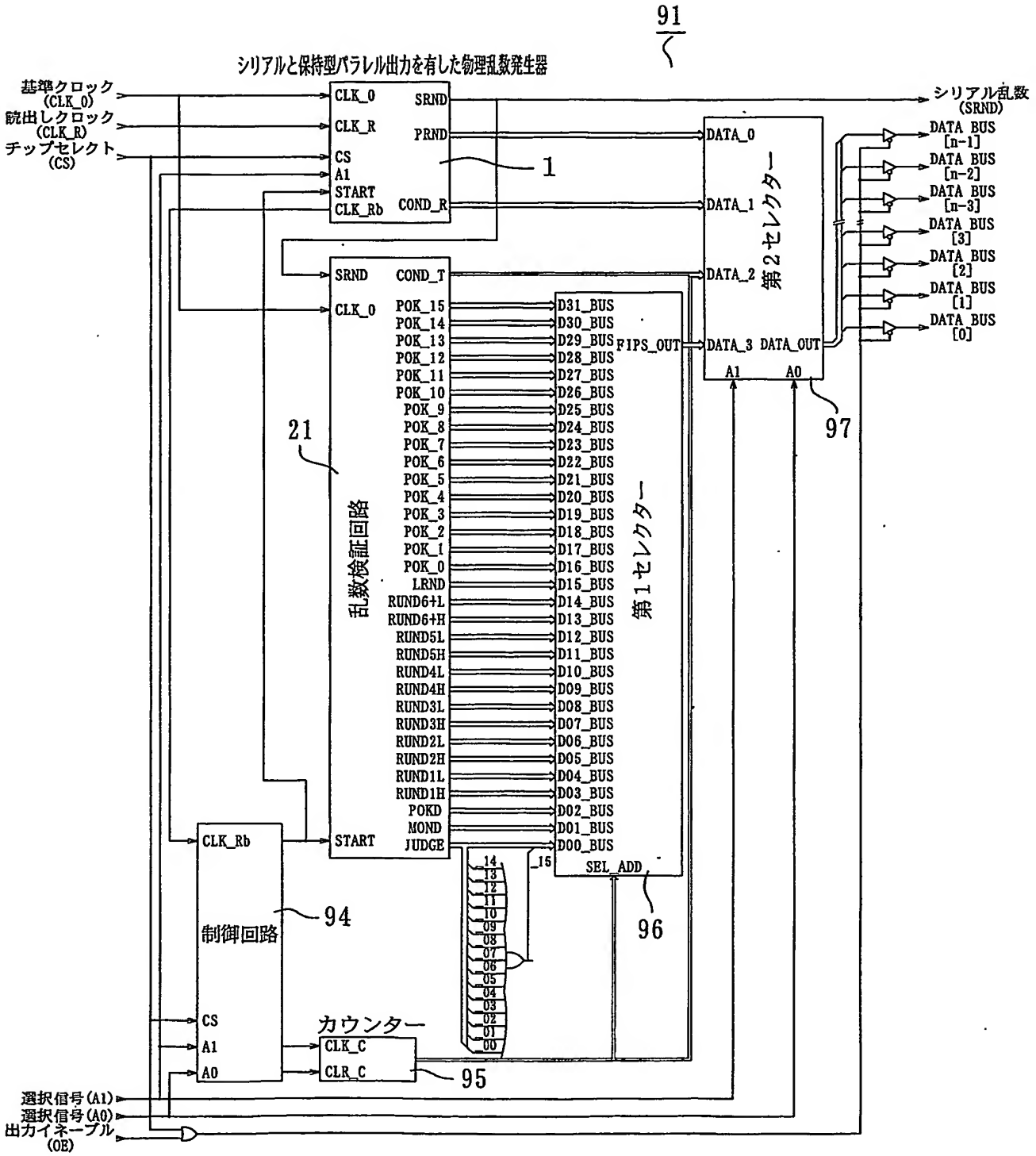

91
シリアルと保持型パラレル出力を有した物理乱数発生器
基準クロック (CLK_0)
読出しクロック (CLK_R)
チップセレクト (CS)
CLK_0
CLK_R
CS
A1
START
CLK_Rb
SRND
PRND
COND_R
1
シリアル乱数 (SRND)
DATA_0
DATA_1
DATA_2
DATA_3
DATA_OUT
第2セレクター
A1
A0
97
DATA BUS [n-1]
DATA BUS [n-2]
DATA BUS [n-3]
DATA BUS [3]
DATA BUS [2]
DATA BUS [1]
DATA BUS [0]
21
乱数検証回路
COND_T
POK_15
POK_14
POK_13
POK_12
POK_11
POK_10
POK_9
POK_8
POK_7
POK_6
POK_5
POK_4
POK_3
POK_2
POK_1
POK_0
LRND
RUND6+L
RUND6+H
RUND5L
RUND5H
RUND4L
RUND4H
RUND3L
RUND3H
RUND2L
RUND2H
RUND1L
RUND1H
POKD
MOND
JUDGE
D31_BUS
D30_BUS
D29_BUS
D28_BUS
D27_BUS
D26_BUS
D25_BUS
D24_BUS
D23_BUS
D22_BUS
D21_BUS
D20_BUS
D19_BUS
D18_BUS
D17_BUS
D16_BUS
D15_BUS
D14_BUS
D13_BUS
D12_BUS
D11_BUS
D10_BUS
D09_BUS
D08_BUS
D07_BUS
D06_BUS
D05_BUS
D04_BUS
D03_BUS
D02_BUS
D01_BUS
D00_BUS
FIPS_OUT
第1セレクター
SEL_ADD
96
14
15
CLK_Rb
制御回路
94
CS
A1
A0
カウンター
CLK_C
CLR_C
95
選択信号(A1)
選択信号(A0)
出力イネーブル (OE)

FIG. 5

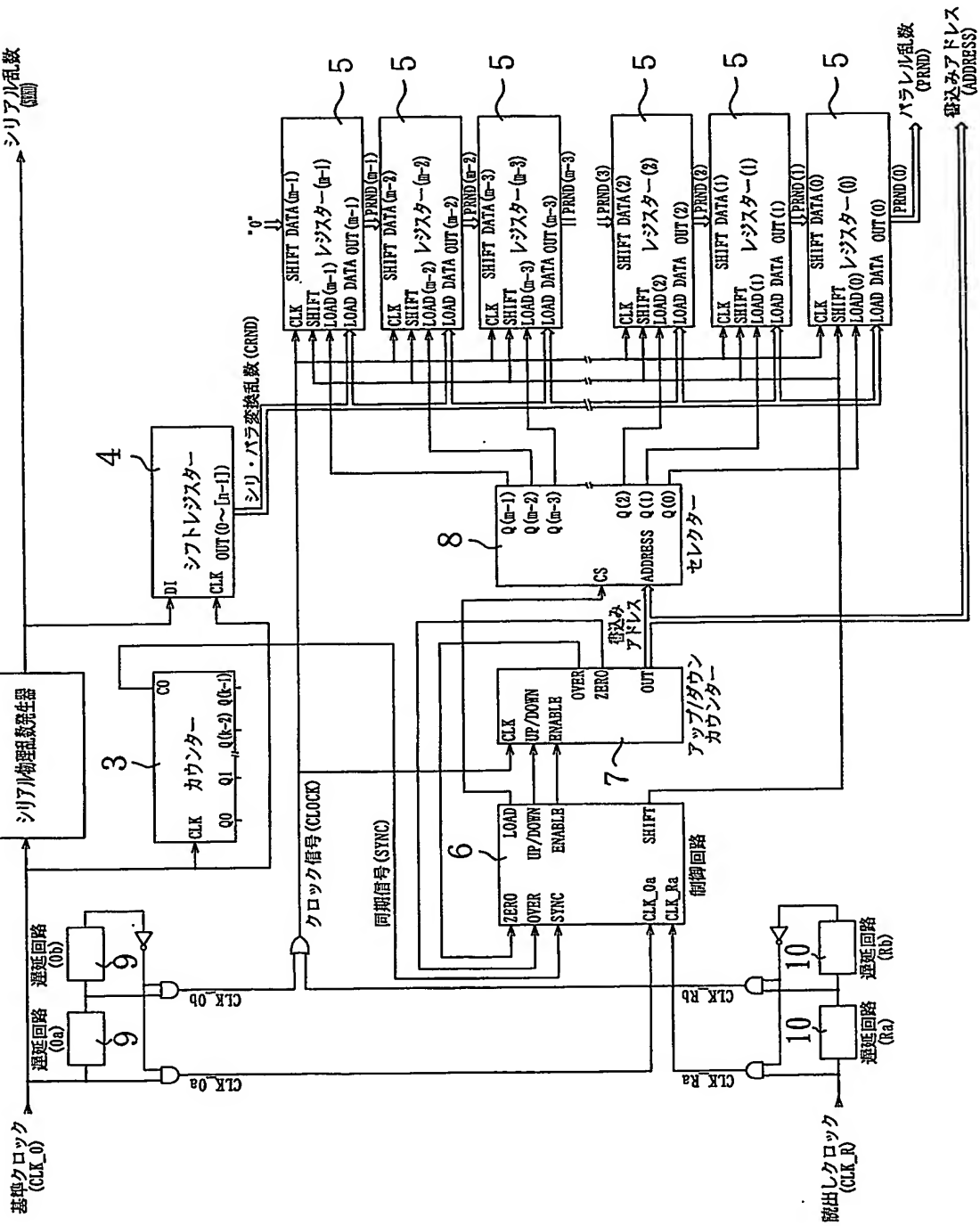

1/7
シリアル乱数 (SRND)
シリアル制御乱数発生器
2
3
カウンター
CO
CLK
Q0
Q1
Q(k-2) Q(k-1)
4
シフトレジスター
DI
CLK
シリ・パラ変換乱数 (CRND)
OUT(0~[n-1])
"0"
5
SHIFT DATA(n-1)
CLK
SHIFT
LOAD
LOAD DATA OUT(n-1)
PRND(n-1)
SHIFT DATA(n-2)
LOAD DATA OUT(n-2)
PRND(n-2)
SHIFT DATA(n-3)
LOAD DATA OUT(n-3)
PRND(n-3)
SHIFT DATA(2)
LOAD DATA OUT(2)
PRND(2)
SHIFT DATA(1)
LOAD DATA OUT(1)
PRND(1)
SHIFT DATA(0)
LOAD DATA OUT(0)
PRND(0)
パラレル乱数 (PRND)
書込みアドレス (ADDRESS)
8
Q(n-1)
Q(n-2)
Q(n-3)
Q(2)
Q(1)
Q(0)
CS
ADDRESS
セレクター
書込みアドレス
アップ/ダウンカウンター
7
CLK
UP/DOWN
ENABLE
OVER
ZERO
OUT
6
LOAD
UP/DOWN
ENABLE
ZERO
OVER
SYNC
SHIFT
CLK_Oa
CLK_Ra
制御回路
クロック信号 (CLOCK)
同期信号 (SYNC)
遅延回路 (Ob)
遅延回路 (Oa)
9
CLK_Ob
CLK_Oa
CLK_Rb
CLK_Ra
10
遅延回路 (Rb)
遅延回路 (Ra)
基準クロック (CLK_O)
読出しクロック (CLK_R)

FIG. 6

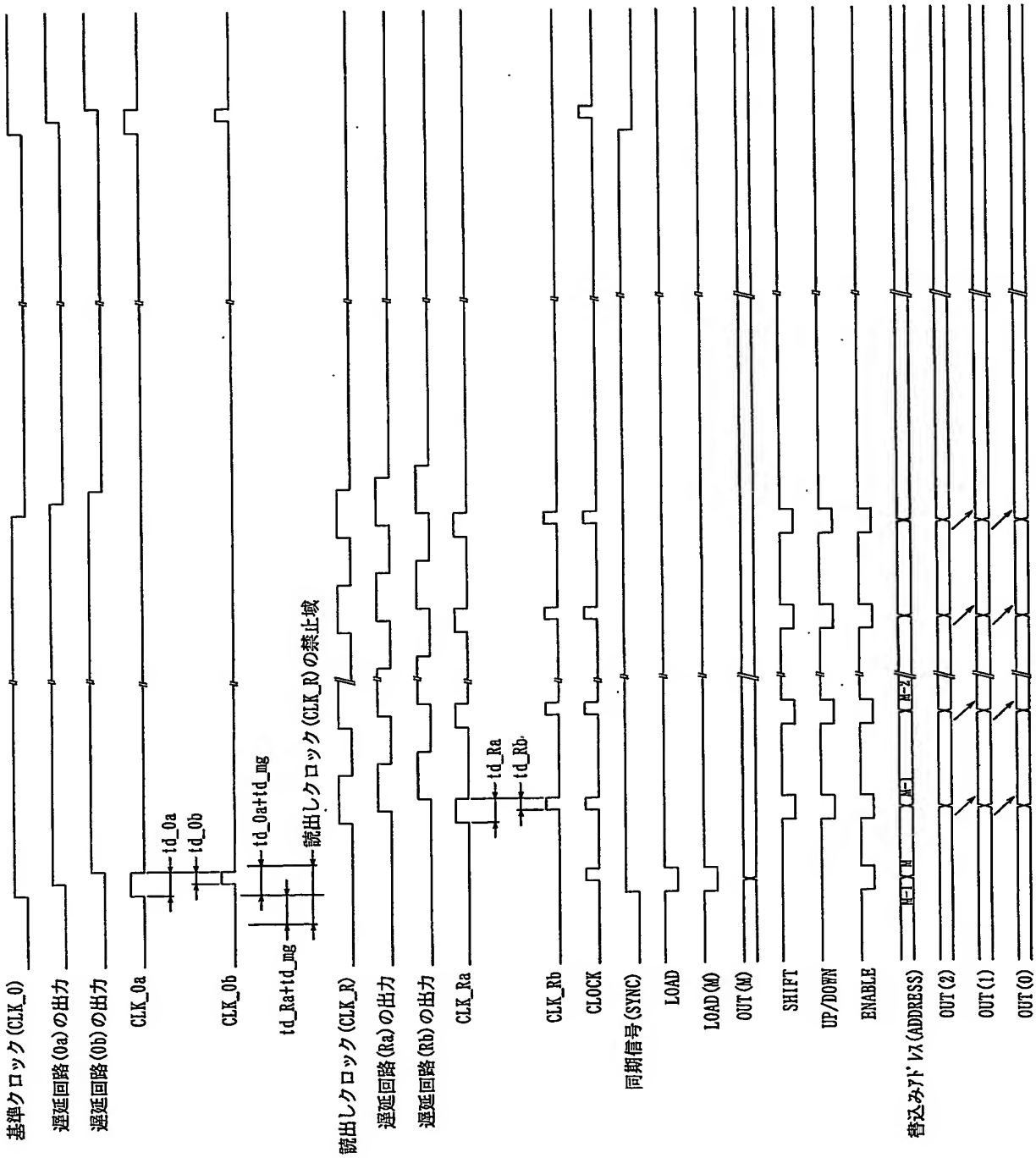

基準クロック(CLK_0)
遅延回路(0a)の出力
遅延回路(0b)の出力
CLK_0a
td_0a
td_0b
CLK_0b
td_0a+td_mg
td_Ra+td_mg
読出しクロック(CLK_R)の禁止域
読出しクロック(CLK_R)
遅延回路(Ra)の出力
遅延回路(Rb)の出力
CLK_Ra
td_Ra
td_Rb
CLK_Rb
CLOCK
同期信号(SYNC)
LOAD
LOAD(M)
OUT(M)
SHIFT
UP/DOWN
ENABLE
書込みアドレス(ADDRESS)
M-1
M
M-2
OUT(2)
OUT(1)
OUT(0)

FIG. 7

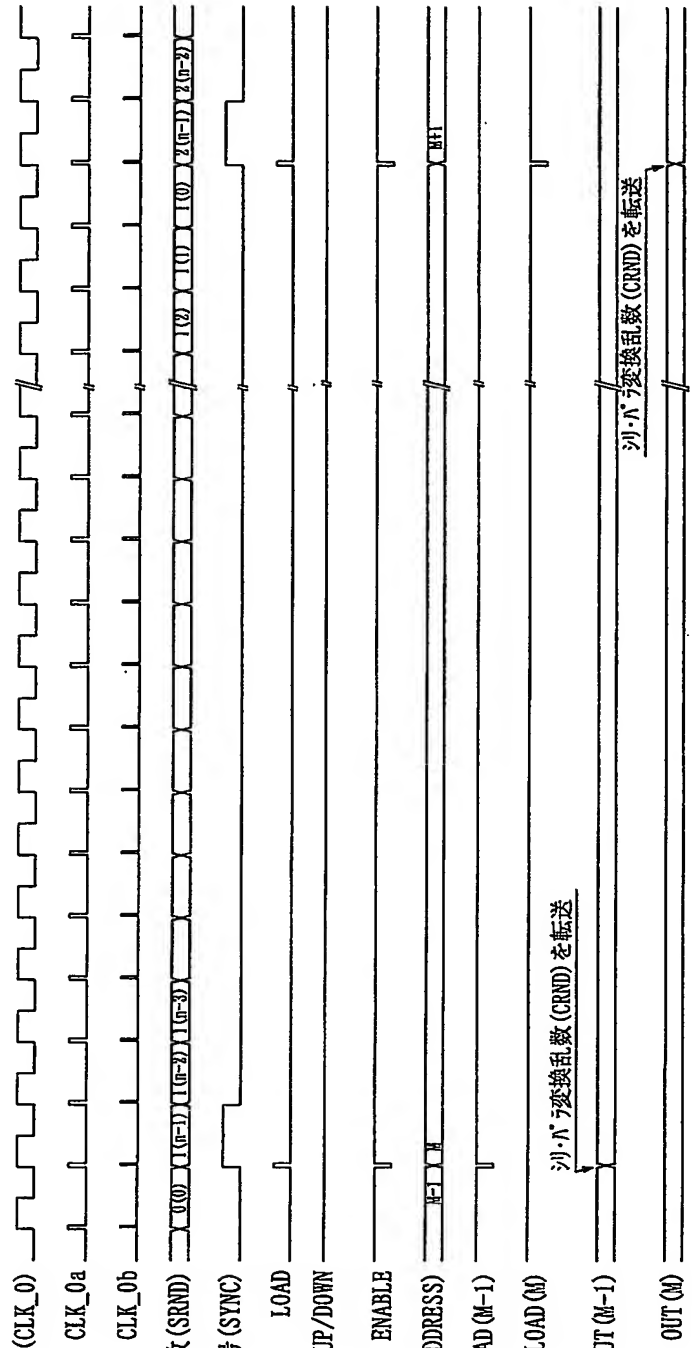

基準クロック(CLK_0)
CLK_0a
CLK_0b
シリアル乱数(SRND)
同期信号(SYNC)
LOAD
UP/DOWN
ENABLE
書込みアドレス(ADDRESS)
LOAD(M-1)
LOAD(M)
OUT(M-1)
OUT(M)
M-1
M
M+1
シリアル乱数(CRND)を転送
シリアル乱数(CRND)を転送

FIG. 8

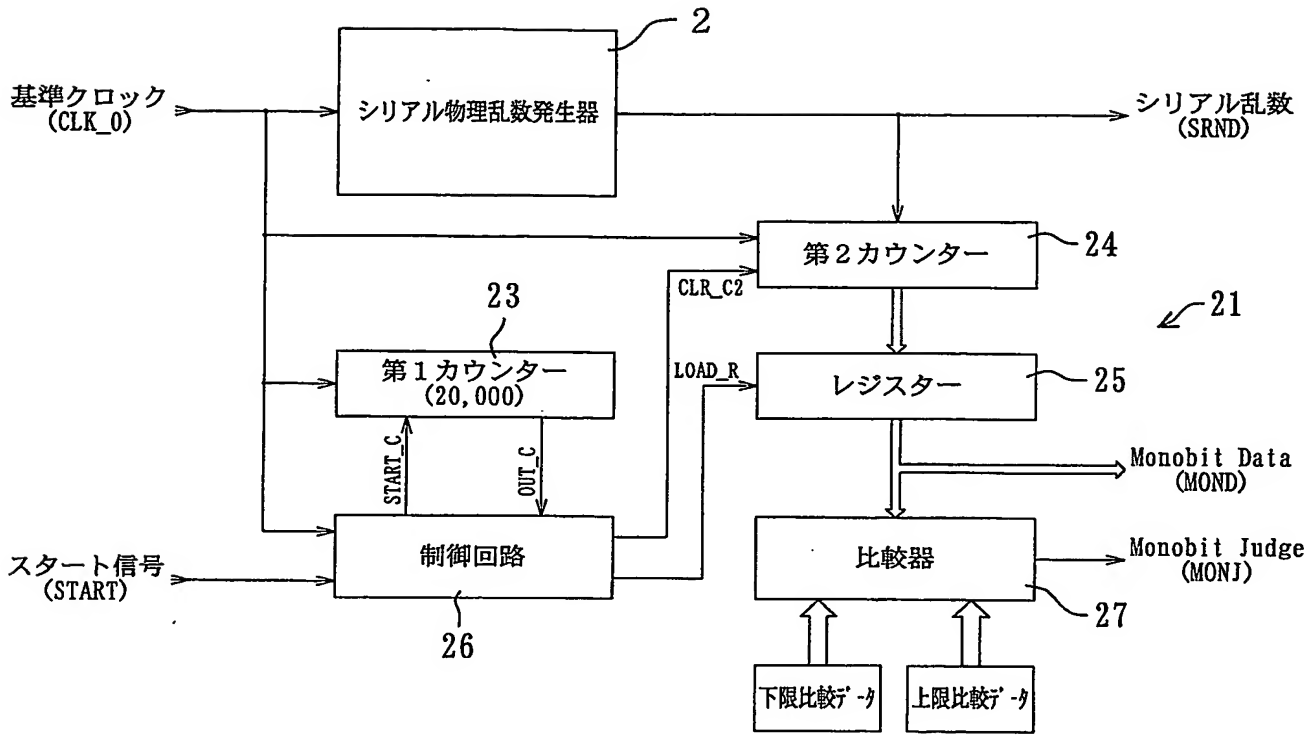

2
基準クロック
(CLK_0)
シリアル物理乱数発生器
シリアル乱数
(SRND)
第２カウンター
24
CLR_C2
21
23
第１カウンター
(20,000)
LOAD_R
レジスター
25
START_C
OUT_C
Monobit Data
(MOND)
スタート信号
(START)
制御回路
比較器
Monobit Judge
(MONJ)
27
26
下限比較ﾃﾞｰﾀ
上限比較ﾃﾞｰﾀ

FIG. 9

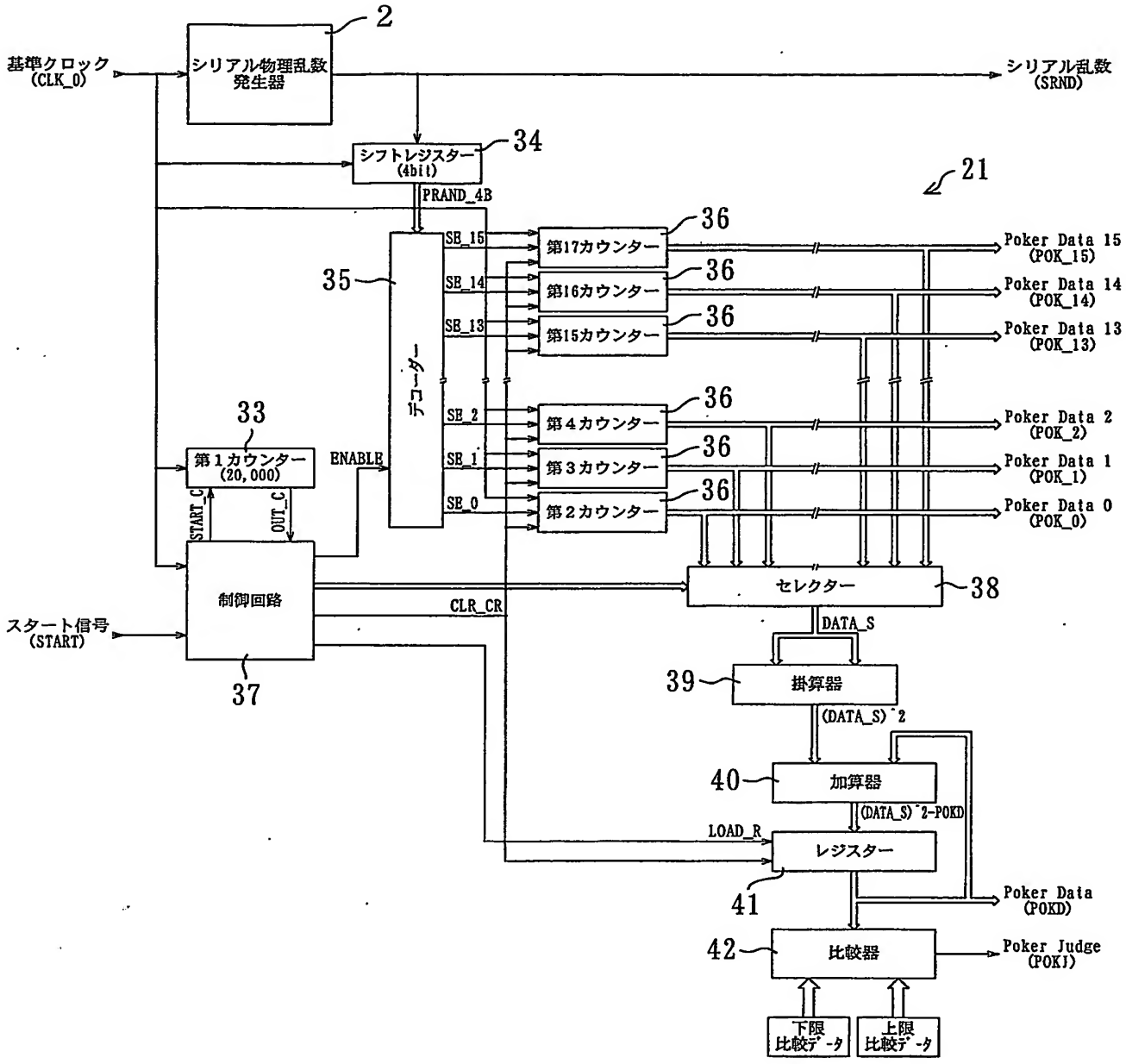

2
基準クロック
(CLK_0)
シリアル物理乱数
発生器
シリアル乱数
(SRND)
34
シフトレジスター
(4bit)
PRAND_4B
21
36
35
SB_15
SB_14
SB_13
SB_2
SB_1
SB_0
デコーダー
第17カウンター
第16カウンター
第15カウンター
第4カウンター
第3カウンター
第2カウンター
Poker Data 15
(POK_15)
Poker Data 14
(POK_14)
Poker Data 13
(POK_13)
Poker Data 2
(POK_2)
Poker Data 1
(POK_1)
Poker Data 0
(POK_0)
33
第1カウンター
(20,000)
ENABLE
START_C
OUT_C
制御回路
スタート信号
(START)
37
CLR_CR
セレクター
38
DATA_S
39
掛算器
(DATA_S)*2
40
加算器
(DATA_S)*2-POKD
LOAD_R
レジスター
41
Poker Data
(POKD)
42
比較器
Poker Judge
(POKJ)
下限
比較データ
上限
比較データ

FIG. 10

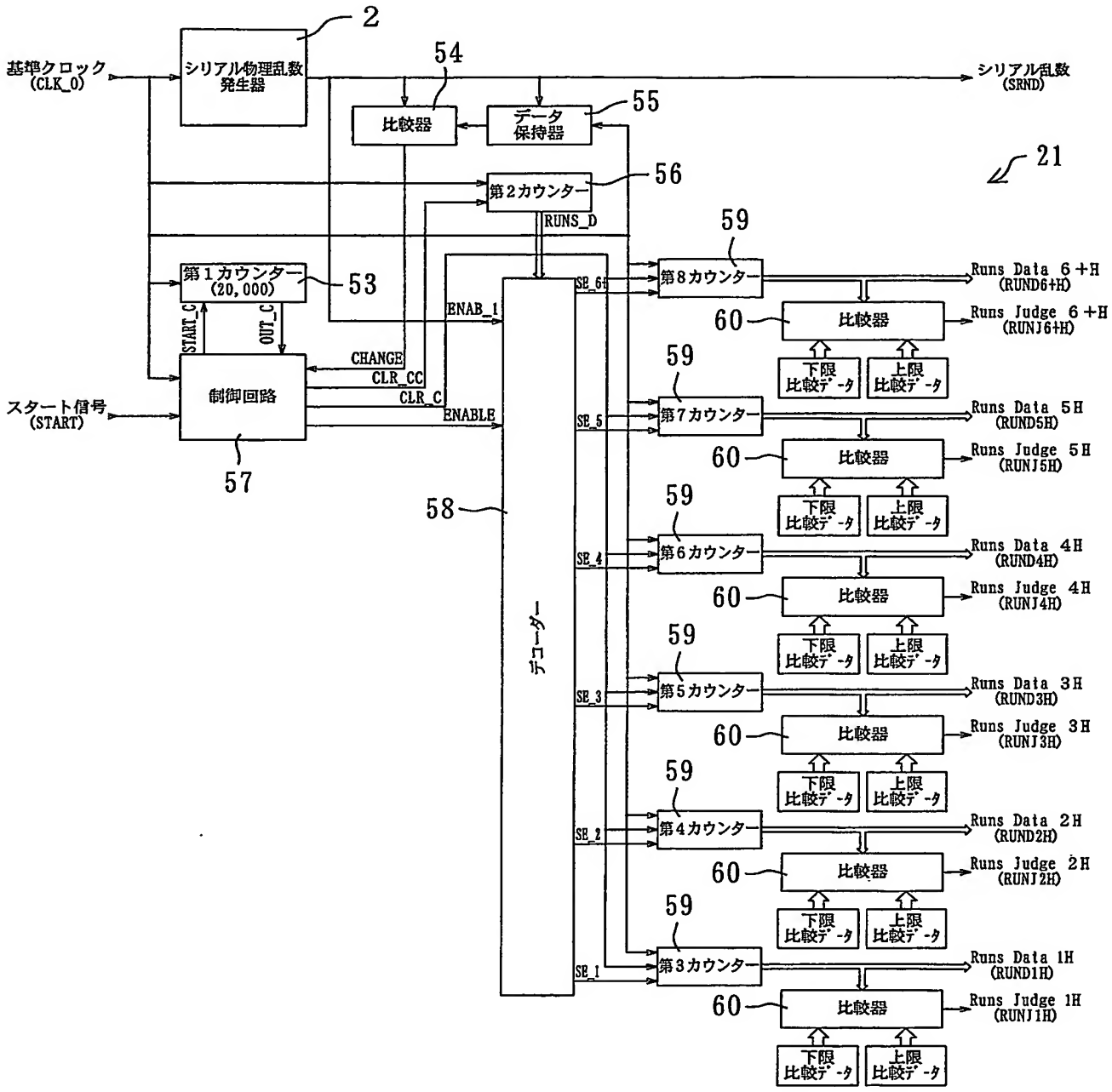

2
基準クロック
(CLK_0)
シリアル物理乱数
発生器
シリアル乱数
(SRND)
54
比較器
データ
保持器
55
21
56
第2カウンター
RUNS_D
59
第1カウンター
(20,000)
53
START_C
OUT_C
ENAB_1
CHANGE
CLR_CC
CLR_C
ENABLE
スタート信号
(START)
制御回路
57
58
デコーダー
SE_6
SE_5
SE_4
SE_3
SE_2
SE_1
第8カウンター
第7カウンター
第6カウンター
第5カウンター
第4カウンター
第3カウンター
60
比較器
下限
比較データ
上限
比較データ
Runs Data 6+H
(RUND6+H)
Runs Judge 6+H
(RUNJ6+H)
Runs Data 5H
(RUND5H)
Runs Judge 5H
(RUNJ5H)
Runs Data 4H
(RUND4H)
Runs Judge 4H
(RUNJ4H)
Runs Data 3H
(RUND3H)
Runs Judge 3H
(RUNJ3H)
Runs Data 2H
(RUND2H)
Runs Judge 2H
(RUNJ2H)
Runs Data 1H
(RUND1H)
Runs Judge 1H
(RUNJ1H)

FIG. 11

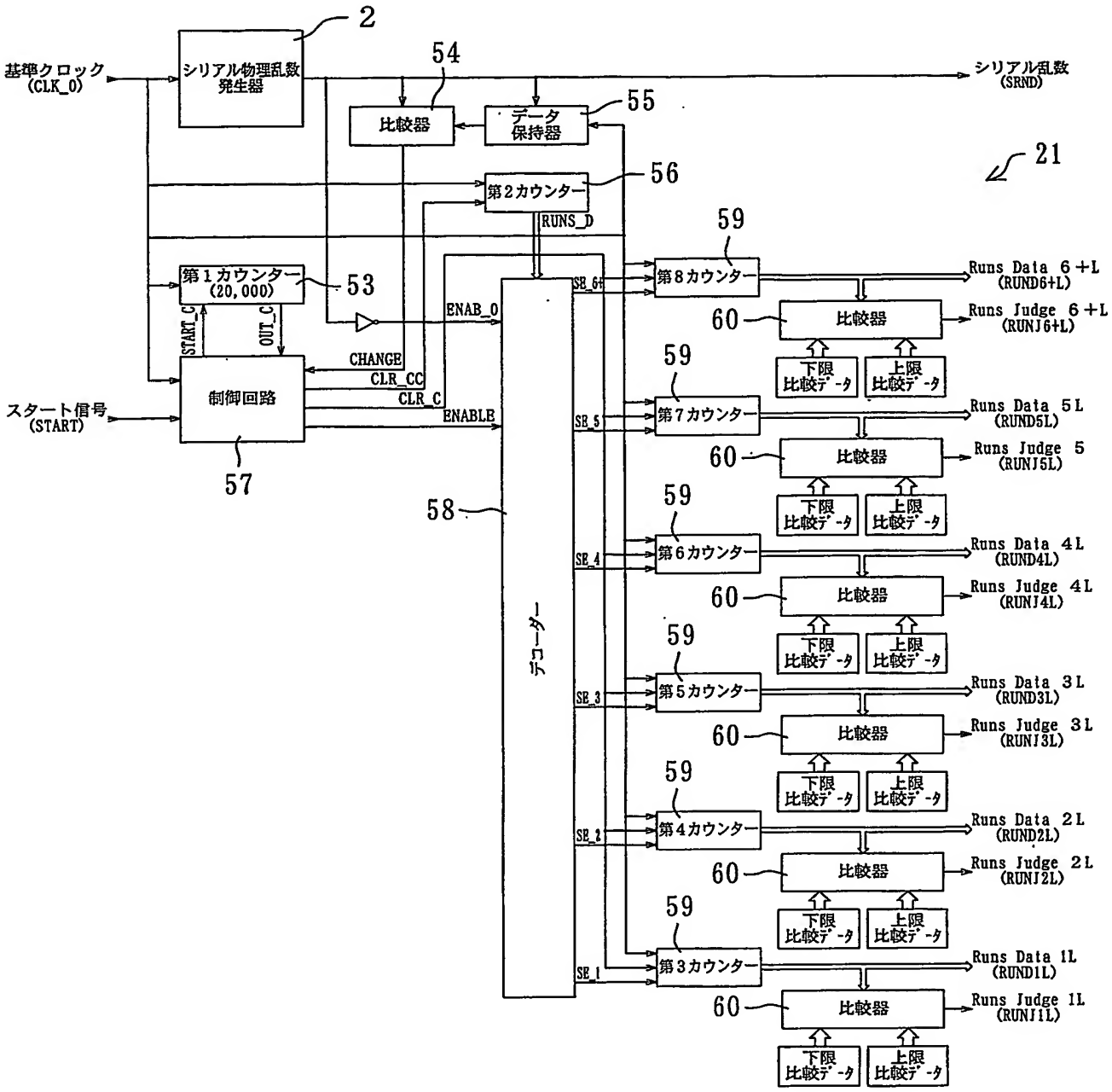

2
基準クロック (CLK_0)
シリアル物理乱数発生器
シリアル乱数 (SRND)
54
比較器
データ保持器
55
21
56
第2カウンター
RUNS_D
59
第8カウンター
Runs Data 6+L (RUND6+L)
60
比較器
Runs Judge 6+L (RUNJ6+L)
下限比較データ
上限比較データ
第1カウンター (20,000)
53
START_C
OUT_C
ENAB_0
CHANGE
CLR_CC
CLR_C
ENABLE
制御回路
スタート信号 (START)
57
58
SE_6
SE_5
SE_4
SE_3
SE_2
SE_1
デコーダー
第7カウンター
Runs Data 5L (RUND5L)
Runs Judge 5 (RUNJ5L)
第6カウンター
Runs Data 4L (RUND4L)
Runs Judge 4L (RUNJ4L)
第5カウンター
Runs Data 3L (RUND3L)
Runs Judge 3L (RUNJ3L)
第4カウンター
Runs Data 2L (RUND2L)
Runs Judge 2L (RUNJ2L)
第3カウンター
Runs Data 1L (RUND1L)
Runs Judge 1L (RUNJ1L)

FIG. 12

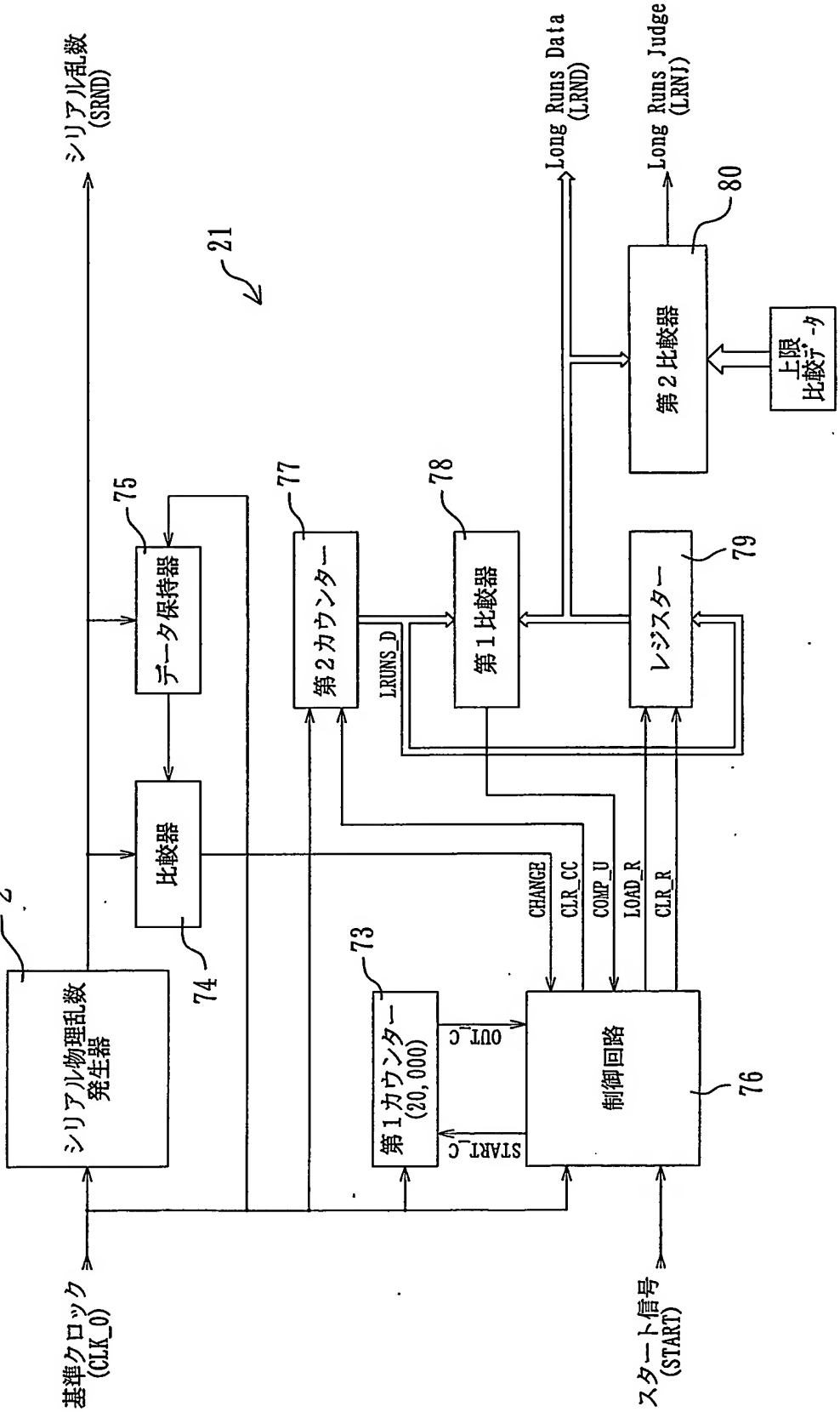

シリアル乱数
(SRND)
21
Long Runs Data
(LRND)
Long Runs Judge
(LRNJ)
80
第２比較器
上限
比較データ
75
データ保持器
77
第２カウンター
78
第１比較器
79
レジスター
LRUNS_D
2
比較器
74
73
CHANGE
CLR_CC
COMP_U
LOAD_R
CLR_R
シリアル物理乱数
発生器
第１カウンター
(20,000)
OUT_C
START_C
制御回路
76
基準クロック
(CLK_0)
スタート信号
(START)

FIG. 13

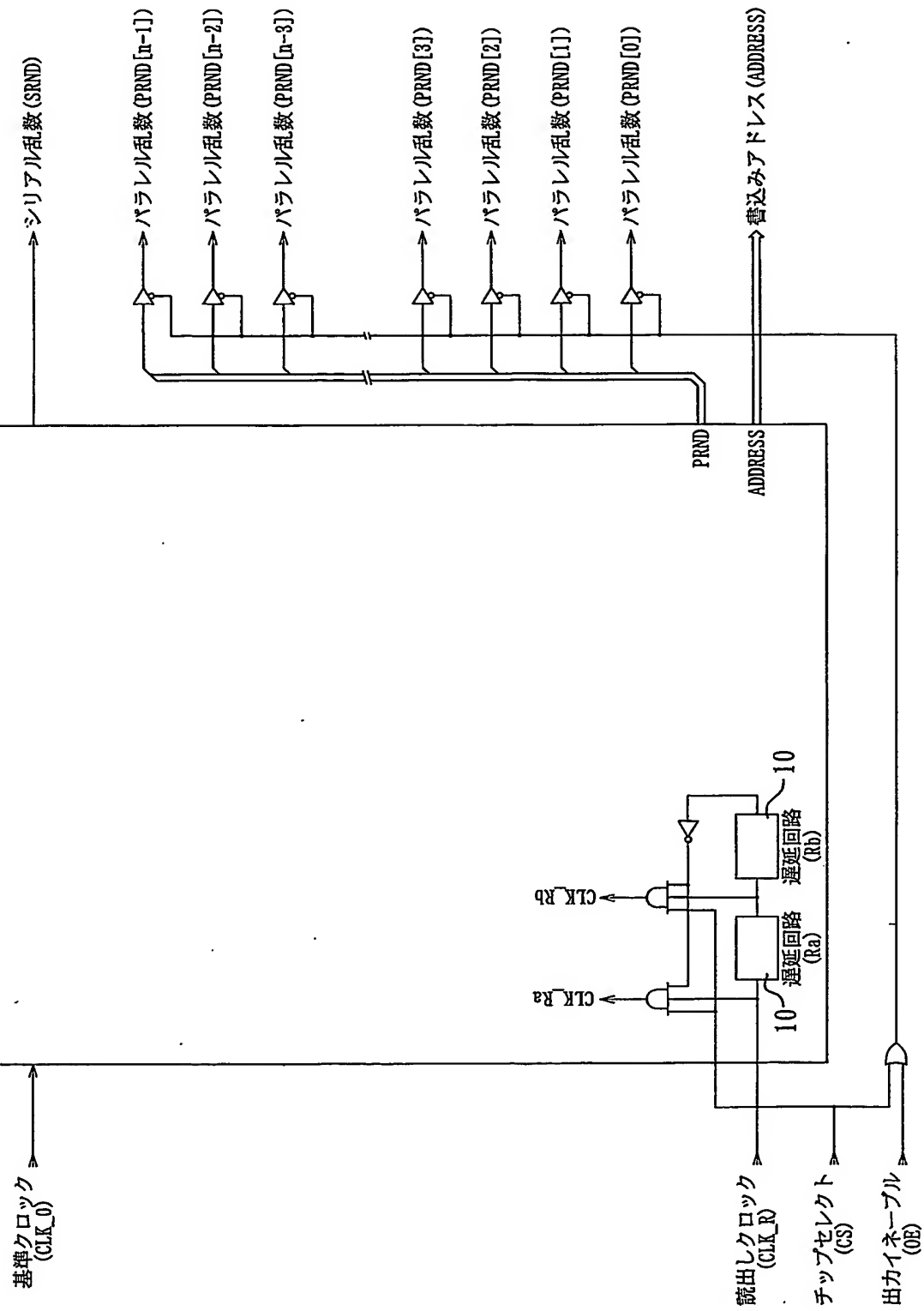

91
1
シリアルと保持型パラレル出力を有した物理乱数発生器
シリアル乱数(SRND)
パラレル乱数(PRND[n-1])
パラレル乱数(PRND[n-2])
パラレル乱数(PRND[n-3])
パラレル乱数(PRND[3])
パラレル乱数(PRND[2])
パラレル乱数(PRND[1])
パラレル乱数(PRND[0])
書込みアドレス(ADDRESS)
PRND
ADDRESS
10
遅延回路(Rb)
10
遅延回路(Ra)
CLK_Rb
CLK_Ra
基準クロック(CLK_0)
読出しクロック(CLK_R)
チップセレクト(CS)
出力イネーブル(OE)

FIG. 14

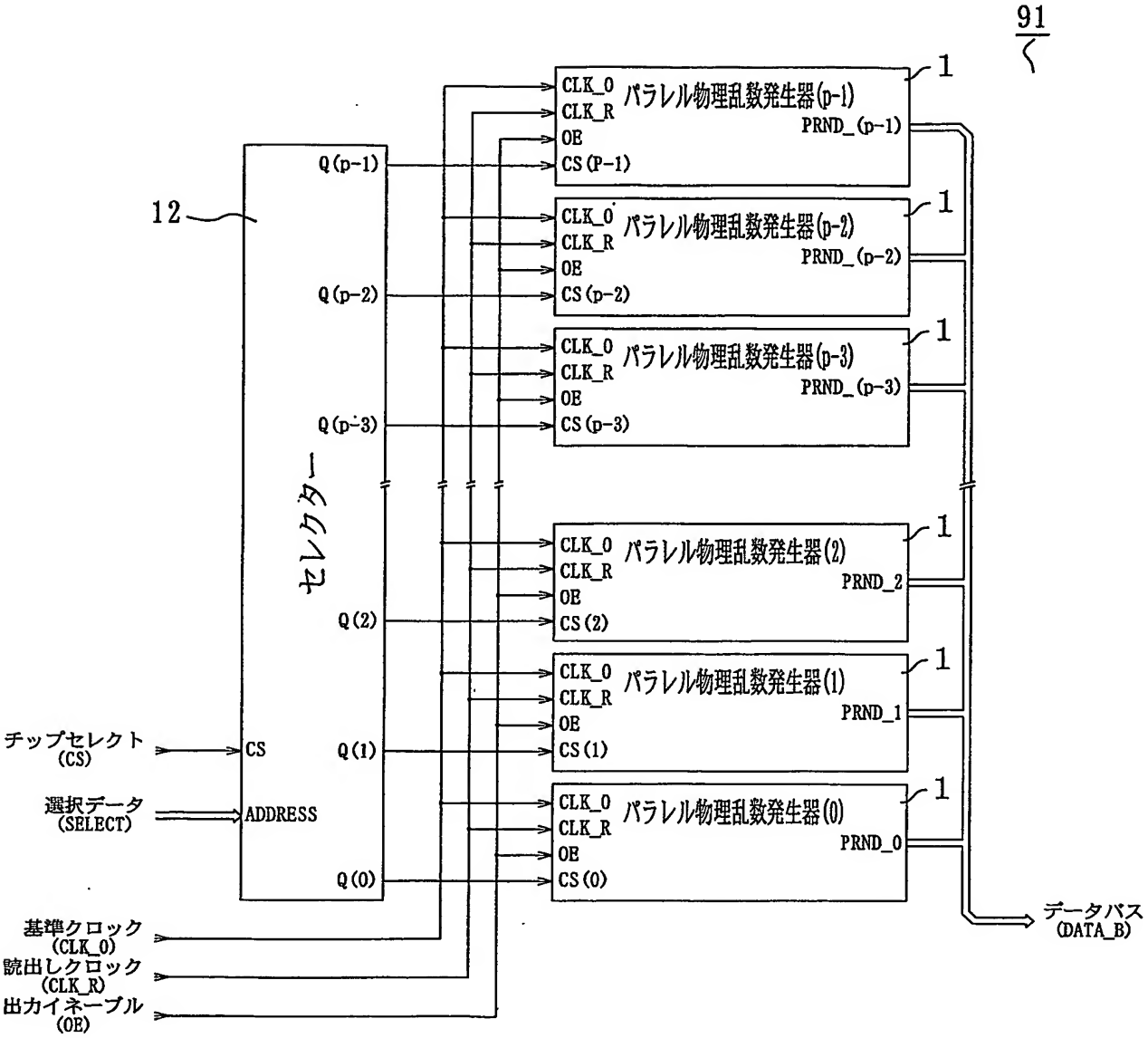

91
12
セレクター
Q(p-1)
Q(p-2)
Q(p-3)
Q(2)
Q(1)
Q(0)
CS
ADDRESS
チップセレクト (CS)
選択データ (SELECT)
基準クロック (CLK_0)
読出しクロック (CLK_R)
出力イネーブル (OE)
CLK_0
CLK_R
OE
CS(P-1)
CS(p-2)
CS(p-3)
CS(2)
CS(1)
CS(0)
パラレル物理乱数発生器(p-1)
パラレル物理乱数発生器(p-2)
パラレル物理乱数発生器(p-3)
パラレル物理乱数発生器(2)
パラレル物理乱数発生器(1)
パラレル物理乱数発生器(0)
PRND_(p-1)
PRND_(p-2)
PRND_(p-3)
PRND_2
PRND_1
PRND_0
1
データバス (DATA_B)

FIG. 15

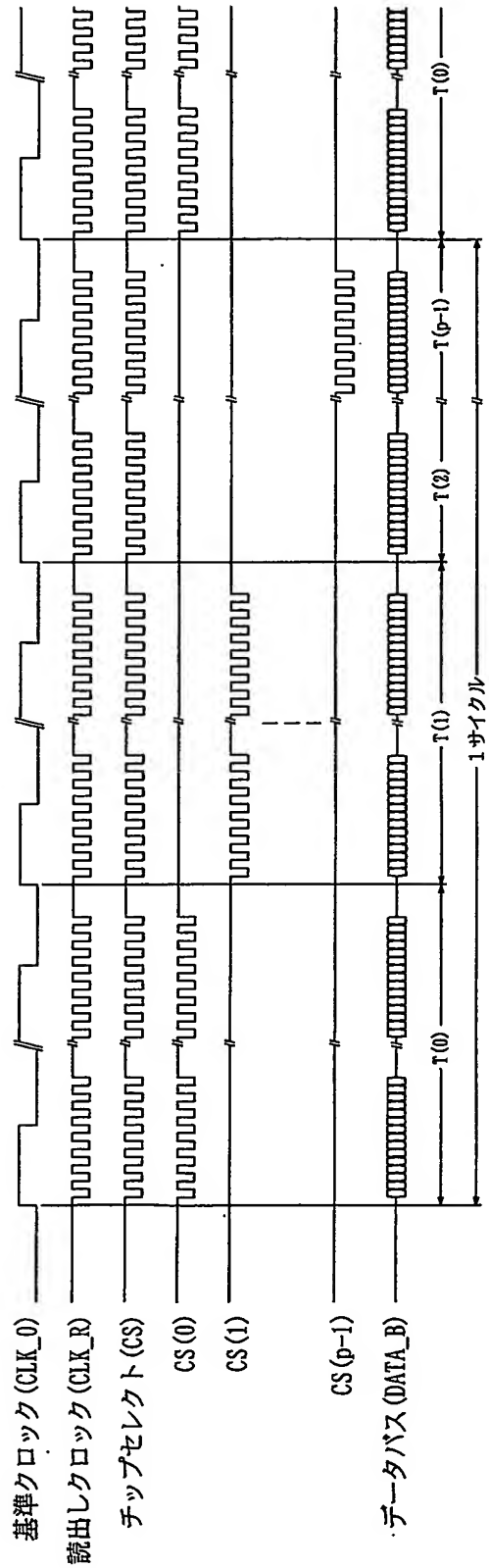

基準クロック(CLK_0)
読出しクロック(CLK_R)
チップセレクト(CS)
CS(0)
CS(1)
CS(p-1)
データバス(DATA_B)
T(0)
T(1)
T(2)
T(p-1)
T(0)
1サイクル

FIG. 16

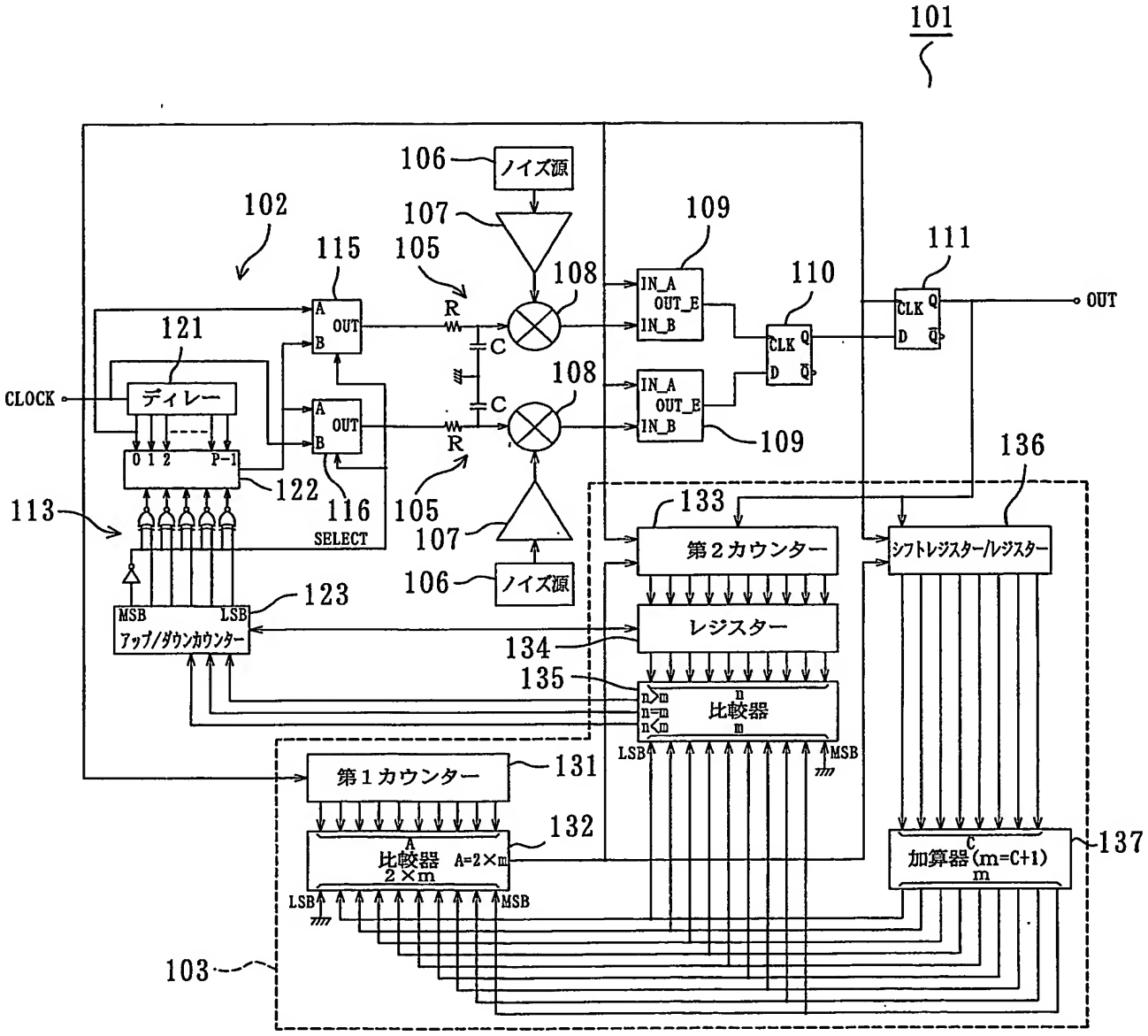

101
102
103
106
ノイズ源
107
105
108
109
110
111
115
116
121
122
123
131
132
133
134
135
136
137
CLOCK
ディレー
OUT
SELECT
R
C
IN_A
OUT_E
IN_B
CLK
D
Q
0 1 2 P-1
MSB
LSB
アップ/ダウンカウンター
第１カウンター
第２カウンター
レジスター
比較器
シフトレジスター/レジスター
加算器(m=C+1)
A=2×m

FIG. 17

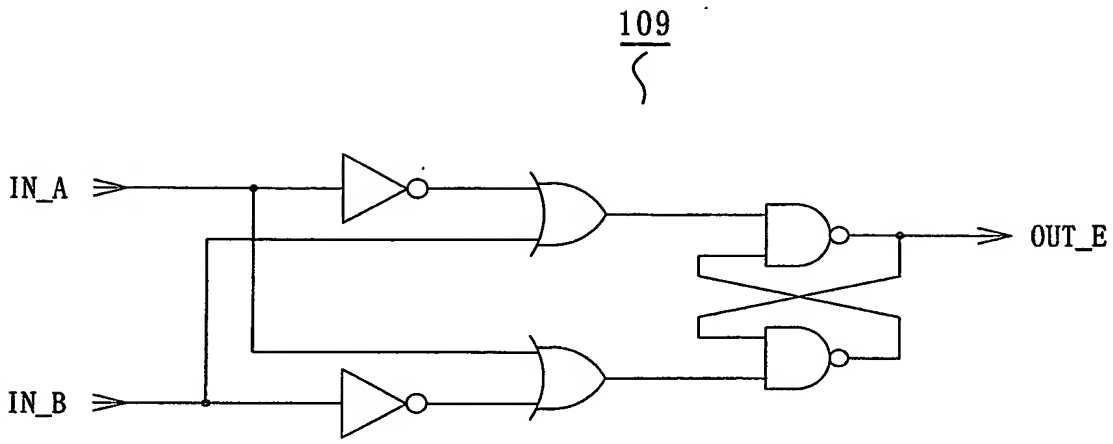


FIG. 18

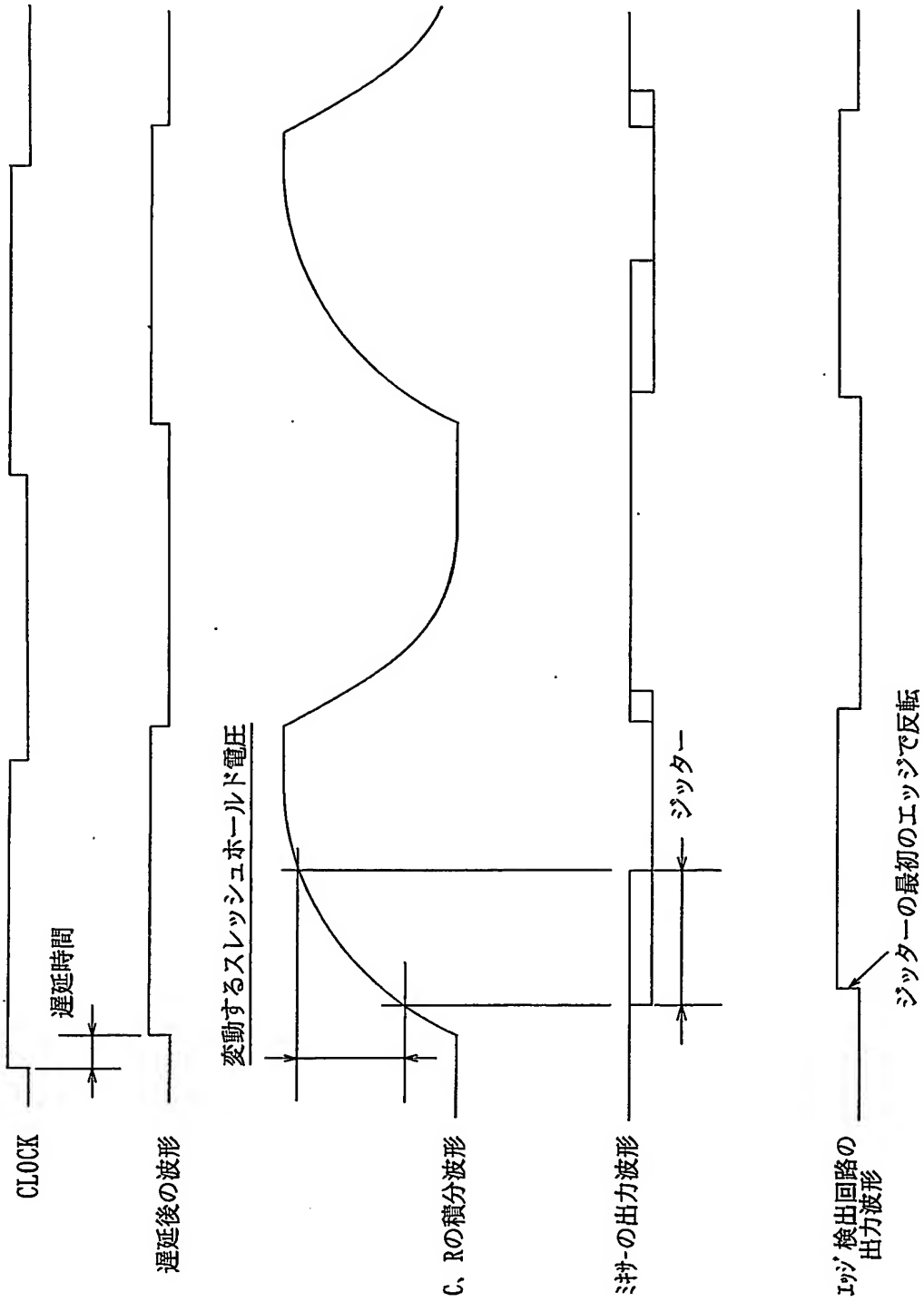

CLOCK
遅延時間
遅延後の波形
変動するスレッシュホールド電圧
C, Rの積分波形
ジッター
ミキサーの出力波形
エッジ検出回路の出力波形
ジッターの最初のエッジで反転

FIG. 19

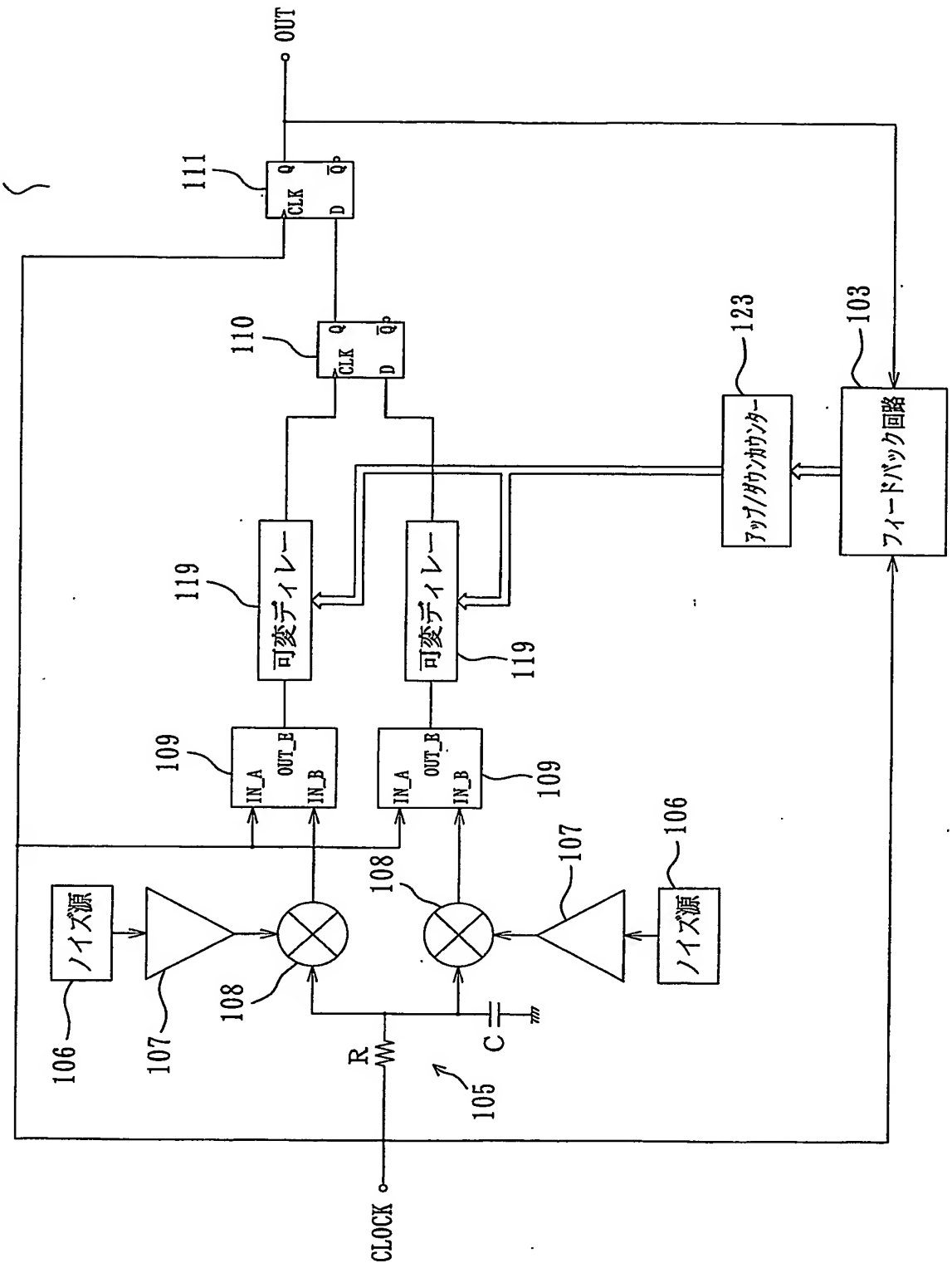

101
OUT
111
CLK
Q
D
110
123
103
アップ/ダウンカウンター
フィードバック回路
119
可変ディレー
109
IN_A
OUT_E
IN_B
OUT_B
106
ノイズ源
107
108
R
C
105
CLOCK

FIG. 20

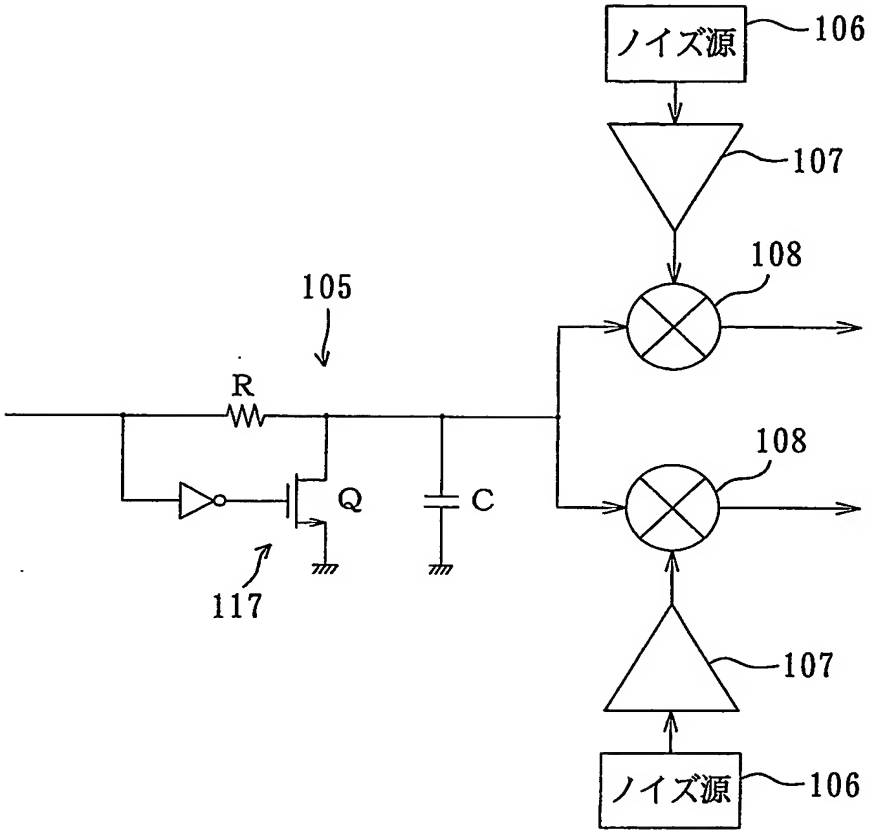


FIG. 21

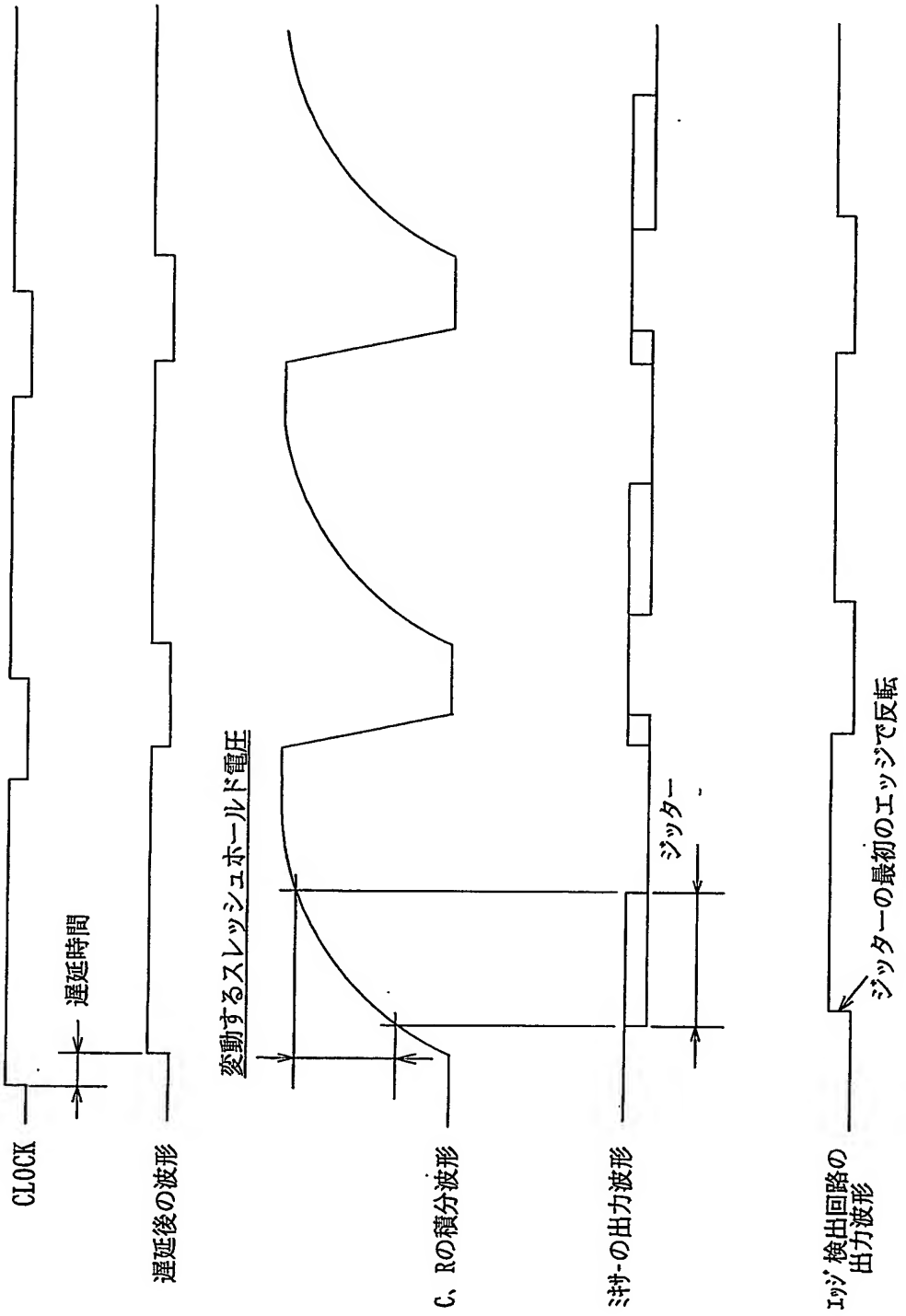

CLOCK
遅延時間
遅延後の波形
変動するスレッシュホールド電圧
C、Rの積分波形
ｼﾐｯﾄ-の出力波形
ジッター
ｴｯｼﾞ検出回路の
出力波形
ジッターの最初のエッジで反転

FIG. 22

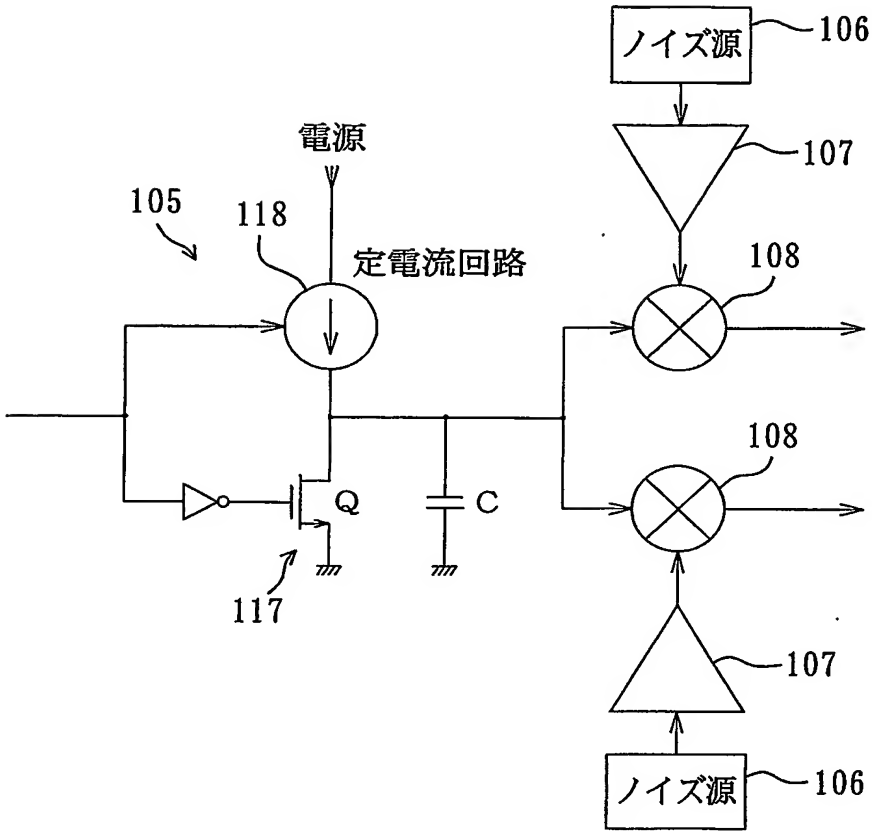
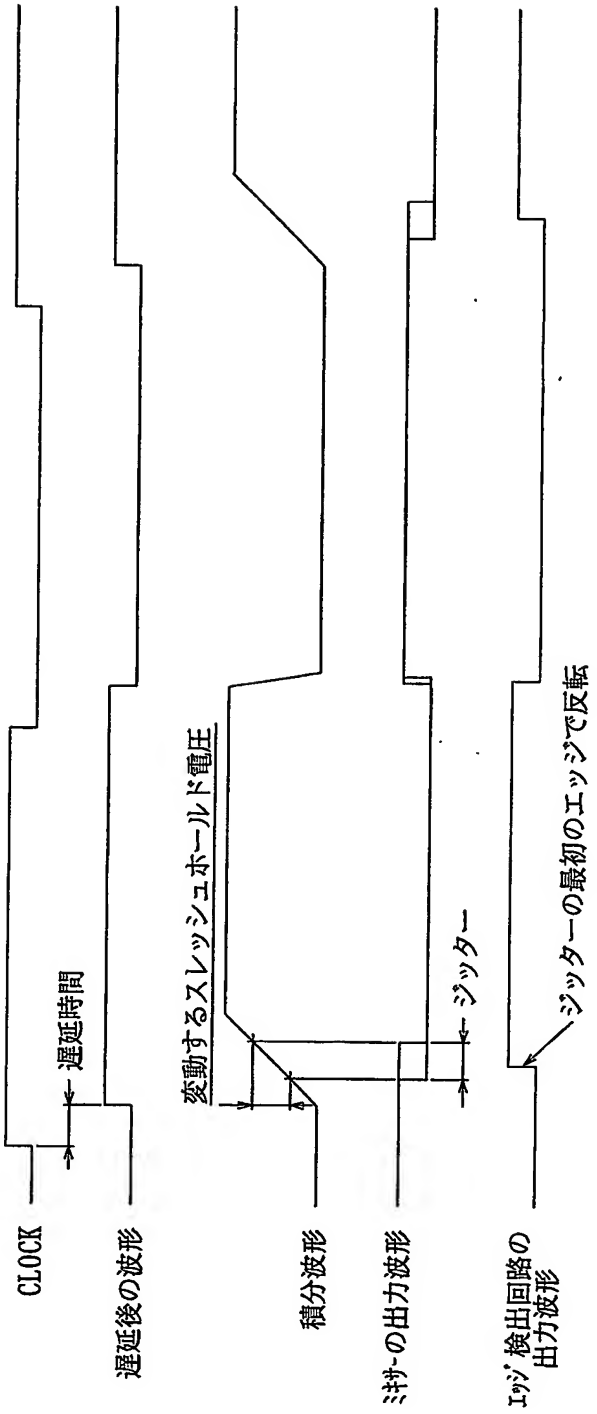


FIG. 23


CLOCK
遅延時間
遅延後の波形
変動するスレッシュホールド電圧
積分波形
ジッター
ﾐｷｻｰの出力波形
ｴｯｼﾞ検出回路の出力波形
ジッターの最初のエッジで反転

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12213

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F7/58, H03K3/84

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 62-109082 A (NEC Corp.), 20 May, 1987 (20.05.87), Full text; all drawings (Family: none)	1-5
Y	JP 1-258130 A (Matsushita Electric Industrial Co., Ltd.), 16 October, 1989 (16.10.89), Full text; all drawings (Family: none)	1-5
A	JP 8-18550 A (NTT Mobile Communications Network Inc.), 19 January, 1996 (19.01.96), Full text; all drawings & EP 680172 A2 & US 5506516 A1	1-5

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 December, 2003 (19.12.03)	13 January, 2004 (13.01.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12213

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 61-97746 A (International Business Machines Corp.), 16 May, 1986 (16.05.86), Full text; all drawings & EP 178432 A2 & US 5046036 A1	1-5
A	JP 9-97170 A (Nikoo-Electronics Co., Ltd.), 08 April, 1997 (08.04.97), Full text; all drawings (Family: none)	6-14
P,A	JP 2003-93620 A (Iwaki Electronics Co., Ltd.), 02 April, 2003 (02.04.03), Full text; all drawings (Family: none)	6-14
P,A	JP 2003-29963 A (FDK Corp.), 31 January, 2003 (31.01.03), Full text; all drawings & WO 02/063767 A1 & CN 1397871 A	9-12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/12213

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 15-19
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

No sufficient mention corresponding to the claims is made in the description.

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1-5 relate to a technique of using part of physical random numbers as the addresses of a selector to uniform physical random numbers.
Claims 6-14 relate to a physical random number generation device that outputs parallel random numbers by means of a plurality of registers and control circuits.
Claim 15 and 16-19 relate to a physical random number generator that generates physical random numbers by using an integrating circuit, a noise source, and an amplifier or the like.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　PCT／JP03／12213

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl' G06F　7／58

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl'　G06F　7／58
　　H03K　3／84

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2003年
日本国登録実用新案公報　1994－2003年
日本国実用新案登録公報　1996－2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　62－109082　A（日本電気株式会社） 1987．05．20，全文、全図（ファミリー無し）	1－5
Y	JP　1－258130　A（松下電器産業株式会社） 1989．10．16，全文、全図（ファミリー無し）	1－5
A	JP　8－18550　A（エヌ・ティ・ティ移動通信網株式会社），1996．01．19，全文、全図 & EP 680172 A2 & US 5506516 A1	1－5

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
19．12．03	13.01.04

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	山崎　慎一	5E	9174
	電話番号　03－3581－1101　内線　3520		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／１２２１３

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　６１－９７７４６　Ａ（インターナショナル・ビジネス・マシーンズ・コーポレイション） １９８６．０５．１６，全文、全図 ＆　ＥＰ　１７８４３２　Ａ２　＆　ＵＳ　５０４６０３６　Ａ１	１－５
Ａ	ＪＰ　９－９７１７０　Ａ（ニコー電子株式会社） １９９７．０４．０８，全文、全図（ファミリー無し）	６－１４
ＰＡ	ＪＰ　２００３－９３６２０　Ａ（いわき電子株式会社） ２００３．０４．０２，全文、全図（ファミリー無し）	６－１４
ＰＡ	ＪＰ　２００３－２９９６３　Ａ（エフ・ディー・ケイ株式会社） ２００３．０１．３１，全文、全図 ＆　ＷＯ　０２／０６３７６７　Ａ１ ＆　ＣＮ　１３９７８７１　Ａ	９－１２

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／１２２１３

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☒ 請求の範囲 ＿＿１５－１９＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
明細書には、上記請求の範囲に対応する十分な記述がない。

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１～５は、物理乱数の一部をセレクターのアドレスとして使用して、物理乱数を一様化する手法に関するものである。
請求の範囲６～１４は、パラレル乱数を複数のレジスター及び制御回路によって出力する物理乱数発生装置に関するものである。
請求の範囲１５及び１６～１９は、物理乱数を積分回路、ノイズ源及び増幅器等を用いて生成する物理乱数発生器に関するものである。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意
☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。